– ArchimedesWhoは、彼の問題は暗号化を使用して解決できると考えているが、彼の問題を理解しておらず、暗号化を理解していない– Roger NeedhamとButler Lampsonが互いに起因している20。  
 そのようなデザインは、3つのかなり異なる背景から来ています。  
 2つ目は、第12章で説明した銀行の世界です。スマートカードは認証トークンとして使用され、HSMはPINとキーを保護するために使用されます。  
 これらすべてのケースで、実際の生活は私たちが予想したよりもやや乱雑であることが判明しました。  
 しかし、エンジニアリングは、攻撃対象領域を減らしたり、フォールトツリー分析を単純化したりするだけではありません。  
この章では、暗号工学の6つの例について説明します60620。  
 完全ディスク暗号化–完全ディスク暗号化、信号プロトコル、Tor、ハードウェアセキュリティモジュール、エンクレーブ、ブロックチェーン。  
 HSMを除くすべてがサイバー犯罪者によって使用されています。  
 マシンの使用中にハードディスク上のデータを暗号化することにより、泥棒がデータではなくハードウェアのみを盗むことができるようになります。  
 それはおそらく次のレベルの複雑さであり、機器の妥協に直面してソーシャルネットワークを可能な限り安全に管理できるようにすることです。  
Torは匿名性を提供することでこれを次のレベルに引き上げます。誰かがあなたのトラフィックを観察して、あなたが誰と話しているのか、どのWebサイトにアクセスしているのかを知られたくない場合です。  
しかし、その上で実行される暗号化アプリは、アプリケーションプログラミングインターフェイスへの攻撃に耐えることができるため、決済アプリケーションに深く絡んでおり、修正が非常に困難です。  
彼らは支払いアプリケーションでHSMを置き換え始めており、Signalでのプライベート連絡先の発見もサポートしています。  
 たとえば、SGXチップからマスター秘密鍵を抽出できれば、エコシステム全体を破壊できます。  
これは、2009年以来、相互に紛らわしい関係者の協力から暗号化メカニズムを使用して出現する共有元帳に基づいてデジタル通貨を作成するプロジェクトです。  
 それでも、暗号化と経済的インセンティブの組み合わせのおかげで、信頼できるコンピューターが何らかの形で出現し、攻撃に成功する可能性のある莫大な金額にも関わらず、動き続けています。  
 いくつかの印象的な事実が現れる。  
20。  
ディスクに書き込むときにデータを暗号化し、再度読み取るときに復号化を行います。  
2。  
 したがって、医師がノートパソコンを電車に乗せたままにしておくと、ハードウェアだけが失われます。医療記録はそうではありません。  
ヨーロッパでは、プライバシー規制当局は一般に、FDEが搭載されたマシンの損失は、データを収集したり、データの件名を強制的に通知する必要があるほど深刻ではないと考えています。  
ただし、表面の少し下を引っかければ、さまざまな不平等があります。  
最初の認証ステップを実行するプラットフォームが必要なため、エンジニアリングは簡単ではありません。  
 それ以外の場合、初期認証はトリッキーです。  
4。  
1、通常のユーザーが設定したものを推測します。  
 FDEをプラットフォームに統合することにより、ベンダーは、オペレーティングシステムの信頼できるブートの信頼できるブート、リカバリキーの設定と管理、およびソフトウェアアップグレード、スワップスペース、デバイスの修復、ユーザーデータのバックアップとリカバリとの非常に複雑な相互作用に対処するための一貫したメカニズムを設計できます。 、デバイスの販売時に出荷時設定にリセットします。  
犯罪者に販売された暗号化電話であるEncroChatには、暗号化されたチャットとVOIPアプリを含む完全に隠されたパーティションがありました。そのような製品については、セクション25で詳しく説明します。  
1。  
 2010年以来、FDE用に設計された特別な操作モードXTS-AESがありました。セクター番号でソルトされた各ブロックを暗号化し、暗号をブロックするためにディスクブロックに適合させるメカニズムを備えています。  
それでも攻撃は続いています。  
 セクション18で説明したとおり。  
 2015年に、ほとんどのAndroidは安全ではないことがわかりました。出荷時設定のリセット機能は、ほとんどのOEMによってひどく設計されており、FDEキーを含む資格情報が中古のデバイスから回復される可能性がありました[1757]。  
セキュリティエンジニアリング608ロスアンダーソン20。  
 シグナルが販売されなくなったらパッチを適用します。  
 そして、付随的な被害があります。  
そして最後に、乱用可能性を考慮する必要があり、そのうち少なくとも2つの重要な種類があります。  
 （もう1つのコンポーネントは暗号通貨で、この章の後半で説明します。したがって、最も単純な暗号化製品でさえ、コンプライアンスとの大きな絡み合いがあり、一見したところ想像よりもはるかに複雑であり、通常はパフォーマンスにペナルティを課し、関連する攻撃が公開されてから何年も経ってからでも、対戦相手に対して脆弱になる可能性があります。  
3Signalスマートフォンが世界中に広がるにつれ、人々はSMSからWhatsApp、Telegram、Signalなどのメッセージングアプリに切り替えました。安価で柔軟性が高く、家族や友人のグループを作成できるようになりました。  
以前はPGPのようなプログラムを使用して電子メールを暗号化することが可能でしたが、（セクション3で説明したように）かなり面倒でした。  
1）そしてニッチな活動のままでした。  
Signalは無料のメッセージングアプリで、最初はMoxie Marlinspikeの名前を使用する男性によって開発されました。  
 モバイルメッセージは非常に機密性が高く、恋人の割り当てから商談まで、外交サミットでの政治的陰謀まですべてが含まれます。それでも携帯電話は、画面が壊れたときに紛失したり盗まれたり、修理のために送られたりすることがよくあります。  
 したがって、Signalプロトコルは、今日の主要な妥協が将来のトラフィックを公開しないという前方の秘密性と、以前のトラフィックも公開しないという後方の秘密性の特性を提供します。  
3。  
このプロトコルには、3つの主要コンポーネントがあります。アリス、ボブ、サーバーの間にキーを設定するための拡張トリプルディーヘルマン（X3DH）プロトコル。秘密鍵が確立されるとメッセージ鍵を導出するラチェットプロトコル。アドレス帳で他の人のシグナルキーを見つけるためのメカニズム。  
したがって、X3DHプロトコル[1227]では、各ユーザーUがIDキーIKUとプレキーSKUをサーバーに発行し、前者を使用して検証できる後者の署名も一緒に発行します。  
 アリスがボブにメッセージを送信する場合、彼女はサーバーからボブのキーIKBとSKBをフェッチし、一時的なDi-e-HellmanキーEKAを生成し、可能なすべての方法でそれらをボブのキーと結合します：DH（IKA、SPKB）、 DH（EKA、IKB）、およびDH（EKA、SPKB）。  
 次に、アリスはボブに自分のキーIKAとEKA、彼女が使用したボブのプリキーのメモ、およびKABを使用して暗号化された暗号文を含む最初のメッセージを送信し、彼がそれを入手したことを確認できるようにします。  
初期のDi-e-HellmanキーKABを指定すると、アリスとボブは2倍ラチェットアルゴリズムを使用して、個々のテキストと通話のメッセージキーを導出します。  
 それは2つのメカニズムを使用します：格納された秘密鍵を更新するための鍵導出関数（KDF）または一方向ハッシュ関数、およびさらにDie-Hellman鍵交換。  
 各メッセージには、関連するチェーンのキーと組み合わされた新しいDi-eHellmanキー部分が含まれ、共有秘密キーはKDFを介して渡されます。  
 目標は、対戦相手がそれらの間のトラフィックにアクセスするために、アリスの電話またはボブのどちらかを絶えず侵害する必要があるということです。  
 チャーリーがサーバーを乗っ取り、ボブの代わりに自分のIKをアリスに送信できる場合、すべての賭けはO↵です。  
AppleのiMessageなどのシステムは、単一のIDキーKIを相手先に送信するだけでなく、MacBook、iPhone、およびその他のAppleデバイスごとに1つのデバイスキーのキーリング全体を送信します。  
 これにより、米国、英国、その他の国で政策の乱れが生じました。その問題については、セクション26で説明します。  
8。  
 Signalはオープンソースになることでこれを未然に防ぎます。  
3。  
 オプションは、ボブの銀行口座からお金を盗もうとした場合とほとんど同じです。  
個人がマウントする最も簡単な攻撃は、おそらくセクション12で説明したSIMスワッピングです。  
4。  
 国家は、高度なハッキングツールを備え、SS7にアクセスできると述べています。FSBが脅威モデルに含まれている場合は、番号がわからない電話を使用することをお勧めします。あなたが知っている、またはそれらがトレースを相互に関連付けるかもしれません-セクション2で説明したように。  
1。  
セクション26で説明します。  
2、信号インテリジェンスのメリットの多くは、メタデータから、誰がいつ誰に電話したのか（または誰が誰といつ電話したかを知ること）から得られます。  
 違法なポリシーを新聞に漏らすことを考えている上級公務員で、あなたがその話を知っている10人のうちの1人なら、Signalを使用したことがあるのはあなただけかもしれません。プライベートな連絡先発見の興味深い革新をもたらします。  
 メッセージングアプリは、アドレス帳へのアクセスを要求し、サーバー上のすべての連絡先を調べて他のユーザーを確認し、それらにメッセージを送信してメッセージを送信できるようにすることで、使いやすさの問題を解決しました。  
 Signalのオリジナルバージョンでは、人々のアドレス帳にある電話番号のハッシュを比較して、誰がそれを使用していたかを調べました。しかし、Christof Hagenandの同僚は、25日間で100のアカウントを使用して、米国の5億5,000万の電話番号すべてをスキャンし、2を発見しました。  
 Signalはプライベートコンタクトディスカバリを実装しました。後でセクション20で説明します。  
 ただし、電話でSignalアカウントを設定すると、プライベートな連絡先の発見でさえ、Signalを使用しているアドレス帳の全員にこの事実がすぐに明らかになります（そして、「Hey、Fredが何かを漏らそうとしている」と言うので、注意してください）リーカーはバーナー電話を現金で買うでしょう。  
 これは、まだ配信されていない暗号化されたメッセージを保存する必要がありますが、どれだけの期間、どのくらいの期間保持されますか？ Signalはグループメンバーシップの記録を保持しますが、今では匿名グループメッセージングの提案があります。これにより、キーが変更されたときに配信されないメッセージを処理する方法についての議論があり、WhatsApp実装は、失敗したものよりも配信を優先することを批判されました。  
4。  
 繰り返しになりますが、テクノロジーができることはそれだけです。グループの1人のメンバーが不誠実である場合、彼らは他の人を裏切ることができます。  
 2016年の選挙後、米国ではかなりの急増があり、2020年に欧州委員会（ヨーロッパの公務員）は、何千もの外交ケーブルを含むサーバーが侵害された後、信号への切り替えを命令しました[399]。  
ユーザーがSignalもメッセージのコンテンツを保持すると想定したため、これは抗議の嵐を巻き起こしました。他のユーザーは、PINで十分な保護ができるとは思っていなかったか、Signalにバンキングに使用したPINを与えたくなかった、または集中化されたデータのアイデアがまったく気に入らなかった。  
 公共の利益のための重要なインフラストラクチャのガバナンスはどのように見えるべきですか？信号はトラフィックの記録を保持しないと主張していますが、NSAからのFISAの令状がそうすることを強制し、それについて嘘をついた場合はどうなりますか？これにより、どのようにしてコミュニケーションを匿名にすることができるかという難しい問題が生じます。  
4TorThe Onion Router（Tor）は、深刻な匿名化を実現するために人々が使用する主なシステムであり、2020年には約200万の同時ユーザーがいます。  
 アリスがイブまたは他の誰も彼女を識別することができない状態でイブのWebサイトを訪問したい場合、ボブが運営するTorリレーへのTLS接続を設定し、ボブが運営するTorリレーへのTLS接続を設定します。 Davidが運営するTorリレー–その「出口ノード」から、AliceはEveのWebサイトへの接続を確立できます[1360]。  
インスピレーションは1981年のDavid Chaumのアイデア、ミックスまたは匿名のリメーラー[410]でした。  
 さまざまな人々が1990年代にこれらについて実験し、適切に機能させるにはさらに3つのものが必要であることがわかりました。  
 第2に、保護するトラフィック（メール、Web、メッセージなど）に合わせて設計する必要があります。  
3Brian Acton、WhatsAppの創設者の1人。  
4。  
 Torが米国の諜報機関に限定されていた場合、それを使用する誰もが標的になります。  
 これは、回路のセットアップと暗号化を処理するだけでなく、Cookie、JavaScript、およびプライバシーに危険を及ぼすその他のブラウザー機能を管理します。  
Torリレー用のソフトウェアもあり、高帯域幅接続でボランティアによって実行されます。 2020年には、約6,000のアクティブリレーが約200万のユーザーにサービスを提供します。  
Torの暗号化およびソフトウェア設計は、さまざまな脅威や不正行為に直面して20年以上にわたって進化し、現在では多くのアプリケーションのコンポーネントとして使用されています。  
 米国国務省がサポートしており、FacebookがTorの最大の目的地です。  
 分類されたドキュメントをリークするために使用できます。  
 警察はこのようなサイトを訪問するためにもそれを使用しているため、オペレーターは自分が警察であることを知りません。  
 しかし、不注意なユーザーから見落とされがちです。  
 2007年9月、誰かが5つのTor出口ノードを設定し、それらを通過するトラフィックを監視し、興味深い記事[1359]を公開しました。しかし、Torのドキュメントでは、出口のトラフィックを読み取ることができることが明記されているため、より慎重な外交官は、当時のGmailと同様に、TLSencryptionをサポートするメールサービスを使用しているはずです。  
これは、2008年にTorブラウザーが導入された主な理由であり、Cookieやその他の指紋印刷メカニズムの追跡機能を制限していました。  
 セクション11。  
3 AOLで識別されたユーザーからの匿名検索の履歴がどのように考えられるかについて説明しました。いくつかのローカル検索（住んでいる場所を示す）といくつかの特別な関心検索（趣味を明らかにする）で十分です。  
 NSAなどのグローバルな敵対者、インターネットの多くのポイントでトラフィックを追跡する場合、少数の交換ポイントをタップするだけで、回路を再構築するのに十分なサンプルを取得できます[1365]。  
 Torは最初から、パスワードの選択に洞察を与えたことを明らかにしました4：ウズベキスタンは「s1e7u0l7c」のようなパスワードを使用し、チュニジアは「チュニジア」とインド大使館「1234」を使用しました。  
4。  
 実際、2014年に、誰か（おそらく諜報機関）がこれを実行していて、プロトコルヘッダーをいじくったシステムに中継することを容易にするためにボランティアをしていることが発見されました[561]。  
第4に、Torは約6,000のリレーのプールを介して接続するため、ファイアウォールがIPアドレスを単純にブロックする可能性があります。  
 このようなブロックを回避するために、ボランティアはTorブリッジを利用可能にします– Torエントリノードはパブリックディレクトリにリストされていません。  
 中国は、国のファイアウォールを迂回する人々が代わりにVPNを使用することを好むようです。これらはよりスケーラブルであるだけでなく、危機の時に完全にシャットダウンするのが簡単です（2020コロナウイルスの発生の初期段階など）。  
本質的に暗号鍵であるタマネギのアドレス。  
 他のタマネギサービスでは、サーバーをハッキングしたり、サプライチェーンを追跡したりしています。  
 また、ゼロデイやサンドボックスエスケープなどの手法を使用して、Torユーザーのブラウザへの攻撃も行われています。  
FDEの場合と同様に、Torはコンプライアンスとの大きな絡み合いを持ち、さまざまな主体が監視を回避し、善悪の両方の法律を回避するのに役立ちます。  
 それは間違いなくパフォーマンスのペナルティを課します– Webサイトは数百ミリ秒ではなく1秒でロードできます。  
 匿名システムには、適切なソフトウェアだけでなく、慎重な運用セキュリティも必要です。  
 Torは、Tor Projectによって維持されています。TorProjectは、2002年に始まったボランティアプロジェクトを正式化するために2006年に設立された米国の非営利団体です。  
 人権に動機付けられた人々の国際社会であり続けています。  
5。  
 大規模なセキュリティにはインフラストラクチャが必要であり、これを主にボランティア活動によって提供するには、契約だけでなく、さまざまな利害関係者のアジェンダ間を変換して価値を交渉できるリーダーが必要です。  
5HSMsバンキングと簿記の章では、銀行がHSMを使用して職務分離ポリシーを実施する方法について説明しました。銀行の単一の人物が顧客のカードの詳細とPINを入手することはできません。  
 暗号通貨業界では、HSMを使用して、重要な資産をサインアウトする可能性のある鍵を保護します。  
 しかし、これだけでは十分ではありません。  
信頼できるコンピューターが信頼性の低いコンピューターと通信するときは常に、信頼性の低いデバイスが嘘をつき不正行為をすることを予期し、予期しないコマンドの組み合わせを使用して境界を調べ、信頼性の高いデバイスをだます。  
 1988年に、LongleyとRigbyは、セキュリティモジュールvendorEracom [1184]の作業を行う際にキータイプを分離することの重要性を認識しました。  
 しかし、2000年にMike Bond、Jolyon Clulow、私がHSM APIが非常に複雑になり、数十の支払いプロトコルバリアントをサポートするための暗号化操作の複雑な組み合わせを含む数百の異なるトランザクションが発生し、それが存在するかどうかについて体系的に考え始めたときに、私たちはペイダートにぶつかりましたそれを壊す一連のHSMトランザクション[71]。  
20。  
1xor-to-null-key攻撃HSMは、銀行のサーバーまたはフィールドのATMから送信されたトランザクションによって駆動されます。  
 ほとんどのキーはデバイスの外部に保存され、1つ以上のマスターキーで暗号化されます。  
セキュリティエンジニアリング615ロスアンダーソン20。  
 HSMS暗号化された作業キーには、機能別に分類するタイプシステムがあります。4。  
 ATMのターミナルマスターキーは同じタイプであり、セクション12から思い出してください。  
1 ATMセキュリティポリシーはデュアルコントロールであるため、銀行は2人のATMカストディアン（デバイスがコミッションされたとき、またはサービス訪問後にキーパッドでキーを入力する支店マネージャーと支店会計士）に個別のキーを生成します。  
 また、暗号化された値を呼び出し元のプログラムに返します。  
攻撃は、キーをそれ自体と組み合わせて、エクスポートできない作業キーとしてマークされた既知のキー（すべてゼロのキー）を生成することでした。  
 すべてゼロのキーで暗号化することにより、王冠の宝石（PIN派生キー）を抽出できます。  
HSMが無効になりました。  
 文書には、デバイスのさまざまなタイプのキーが何をすることになっているのかが明記されていませんでした。エクスポートできない作業キーは、「暗号化されたアンダーマスターキー14および15で提供されるキー」として説明されただけで、そのようなキーを別のキーの下で暗号化するトランザクションの影響はすぐにはわかりませんでした。  
そこでマイクボンドは、デバイスで使用されている主要なタイプの正式なモデルを構築し、すぐに別のフローを発見しました。  
 混乱していましたか？最初は誰もがそうでした–現代のAPIは非常に複雑すぎて、バグをカジュアルな検査で明らかにすることはできません。  
 最新のHSMには強力なタイピングがあり、キーについて正式に推論するのが容易になります。  
5。  
 当時のトップターゲットは、IBM製品の4758 [951]でした。  
 これは、後方セキュリティ攻撃エンジニアリング616Ross Anderson20に対して脆弱であることが判明しました。  
 HSMS互換性[279]。  
この優れたアイデアは下位互換性をもたらしました。左のキーを右のキーと同じに設定すると、暗号化はシングルDESに戻ります。  
 シングルDES鍵の「左半分」と別のDES鍵の「右半分」を取り、それらをまとめて真のTriple-DES鍵にして、これを使用して他の鍵をエクスポートできます。  
 今ではそれほど難しくはありませんが、2002年にはまだかなりの作業でした。  
 その世代のHSMには、キーの「チェック値」がありました。ゼロの文字列を暗号化することによって計算された、各キーの一方向ハッシュです。  
 （たとえば）240個のキーとそのハッシュのテーブルを事前計算します。  
 これには約216回のハッシュが必要で、1時間程度かかります[447]。  
20。  
3差分プロトコル攻撃4758のバグが修正され、ATMの最近のモデルでは、自動登録用の公開鍵メカニズムが提供されています。  
 そして、まだまだたくさんあります。  
 多くのHSMは、特定のアプリケーション向けに調整されたトランザクションをサポートしています。最大の市場セグメントはカード決済をサポートすることです。ここでは、前払いユーティリティメーター、認証機関、さらには核の指揮統制のためのHSMも考えられます。  
セクション12で説明しました。  
2顧客が暗号化されたPINをキャッシュカードに書き込んだばかりの銀行がどのように攻撃されたのか。顧客が口座番号を別の番号に変更し、PINを使用してその口座を手に入れることができるためです。  
 しかし、誤ったアカウント番号がPINブロックと共に送信された場合、HSMはそれを復号化し、アカウント番号をxorします。結果が10進数でない場合、エラーメッセージを返します。  
 現在、特別なものがあります6PIN送信用の4つの異なるPINブロック形式があり、そのうち3つにはPANも含まれています。さらに、PIN検証値（PVV）という形式もあります。これは、銀行がVISAやマスターカードなどのスイッチに代わってPIN検証を行う場合に、銀行から送信されるPINとPANの一方向の暗号化です。 ownSecurity Engineering617Ross Anderson20。  
 PIN変換に関するHSMのHSMSPCIルール[977]。  
その後、Mike BondとPiotr Zielinskiがさらに攻撃を分類しました。  
3。  
 最初の4つは10進数に変換されますが、ほとんどの銀行は10を法とする16進数を使用してこれを行いますが、すべての銀行がそうするわけではありません。  
 これは大きな間違いでした。  
e。  
 次に、テーブル1000000000000000を使用して呼び出しを繰り返します。  
 数十の問い合わせがあれば、PINを推定できます。  
 実際の唯一の解決策は、自社の銀行の10進法化テーブルがハードコードされたマシンに対して、HSMベンダーに追加料金を支払うことでした。  
哲学的レベルでは、これはロバストで安全なマルチパーティ計算（一方の当事者からの秘密情報を使用する計算だけでなく、敵対者が操作できるいくつかの入力も使用する計算）を設計する難しさを示しています。実用的なレベルでは、APIが時間とともに失敗する主な理由の1つを示しています。  
20。  
4EMV攻撃2000年代初頭にAPI攻撃の最初の波が発表された後は、HSM設計者は新しいトランザクションの追加についてより慎重になると考えていました。  
たとえば、スマートカードと銀行HSMの間の安全なメッセージ送信をサポートするためにEMVCoから注文されたHSM機能は、すべてのEMV準拠HSMに悪用可能な脆弱性を導入しました[22]。  
 そのため、EMVCoはトランザクションを定義し、サーバーがHSMにコマンドを送信して暗号化システムを停止できるようにするキーのセキュアメッセージングを停止しました。  
しかし、これは機能しません。0123456789012345、1123456789012345などです。  
5。  
暗号化はCBCまたはECBモードにすることができ、テキストメッセージは可変長にすることができます。  
 次に、そのバイトは、1バイト長い一連のメッセージを送信することで決定できます。追加のバイトは、キーバイトが見つかるまで、256の可能なすべての値を循環します。  
5。  
 （この規格は悪名高く、実装が困難です。  
 彼らは認証機能にパッチを当てることができたため、asadminをHSMにログインし、キーを読み取るツールをインストールすることができました[203]。  
20。  
6 HSMリスクの管理ある時点で、誰かが市場にあるすべてのセキュリティモジュールの少なくとも1つのバージョンに対する攻撃を発見しました。  
 人々は壊れるまでAPIをより複雑にします。  
 他のシステムと同様に、構成管理は厳しくする必要があり、ベンダーのソフトウェアパッチを迅速に適用する必要があります。  
専門企業はHSM管理システムを提供しており、これらが最終的に大手クラウドサービスプロバイダーに組み込まれるかどうかを確認する必要があります。  
 もちろん、PIN管理アプリに本質的なAPIの脆弱性がある場合、これらは従来のオンプレミスHSM、クラウドデータセンターのHSM、またはエンクレーブで実行されているかどうかに依存しません。  
この警告が表示されたら、今度は飛び地を見てみましょう。  
6。  
6エンクレーブエンクレーブはHSMに似ており、信頼できない人が操作するマシンで安全に計算を実行できるプラットフォームを提供することを目的としています。  
 この提案されたアーキテクチャでは、CPUが暗号化されたコードを実行し、キーは別のTrusted Platform Module（TPM）チップに格納されます。  
3。  
TrustZoneは通常、最新のAndroidフォンの中心にあるシステムオンチップ（SoC）に実装されていますが、その信頼境界は通常、マザーボード全体です。エンクレーブデータは、バス上およびDRAMチップ内でクリアに使用できる場合があります。  
 どちらの場合も、ハードウェア攻撃は本当の懸念事項ではありません。  
7。  
 2015年まではクローズドシステムであり、OEMの署名がある場合にのみTrustZoneでコードを実行できました。  
 さらに、コードは製品が使用するSoCによって異なります。  
 ベンダーがクローズドプラットフォームについて行うセキュリティの主張を評価することも困難です。  
2015年に、インテルはSGXを発売しました。そのアクセス制御の側面については、セクション6で説明しました。  
1。  
 AWS、Azure、Googleなどのサービスでシステムを実行する方が安くなります。仮想化によりリソースを効率的に共有できるため、データセンターやシステム管理者などのコストを数千人の顧客にわたって償却できます。  
 ハイパーバイザーソフトウェアの技術的な悪用などにより、機密データがクラウドサービスの他のテナントに漏洩しないようにするにはどうすればよいですか？このような製品には、毎年数十のバグが修正されています[479]。  
 これらの懸念があるため、SGXのセキュリティ境界はチップ自体の境界です。  
 CPUのハードウェアは、機密性と完全性の両方を保護します。  
セキュリティエンジニアリング620ロスアンダーソン20。  
 重要な暗号化メカニズムはソフトウェアの証明であり、これにより、CPUは、実行可能なソフトウェアの所有者に対して、信頼できるハードウェア上で変更を加えることなく認証を行うことができます。  
 エンクレーブの初期化、アドレス変換、ページの削除、例外処理などの詳細は非常に複雑です。説明と分析については、Vic-tor CostanとSrini Devadas [479]を参照してください。  
 特にメルトダウンとスペクターがセクション19で説明したサイドチャネル攻撃の一時的な実行ファミリーを導入して以来、複数のサイドチャネル攻撃もあります。5。  
ここで私の懸念は、エンクレーブをサポートするために使用される暗号と、その上で実行されるソフトウェアを証明すること、およびアプリケーションの他の暗号または暗号サポートのプラットフォームとしての適合性です。  
 各チップにはヒューズがあり、その中にファブがシールシークレットとプロビジョニングシークレットを書き込みます。前者はIntelには知られていませんが、後者は知られています。  
 プロビジョニングシールキーは永続的であるため、コンピューターが所有者を変更するとき、インテルは知る必要がありません。  
これらの操作は、特権起動エンクレーブ（LE）で行われます。  
 各エンクレーブの作成者はCAになり、公開キー、製品ID、およびバージョン番号を持っている各エンクレーブを認証します（シークレットの移行は、より高いバージョン番号にのみ許可され、ロールバックはサポートされません）。  
1つの問題は、1つのチップのMDKが（どのCPUでもどこでも）妥協すると、同じグループ内のすべてのCPUの認証セキュリティが壊れることです。  
 Intelも同じように脆弱です。MDKの明確な価値を考えると、SGXの保護メカニズムの外にSGXエンクレーブを作成できます。  
 すべての証明はIntelによって不透明に行われ、ユーザーは単に結果を信頼する必要があるため、これらのグループがどれほど大きいかはわかりません。  
10SGXはキャッシュタイミング攻撃を防御しないため、エンクレーブコードを作成する場合、データ依存ジャンプを使用できません。  
セキュリティエンジニアリング621ロスアンダーソン20。  
 ENCLAVES今、実際の仕事をしているいくつかのSGXシステムがあります。  
 その開発者は、Signalブログ[1226]でソースコードを開発する難しさについての広範な議論とともに公開しました。  
 どのようにして洞察を持たずに大きなソーシャルグラフを作成できますか？アイデアは、クライアントが飛び地に連絡し、それが適切なソフトウェアを実行していることを確認し、連絡先を送信して、誰がユーザーでもあるかを確認できるというものです。  
メモリアクセスパターンを介した情報漏えいを防ぐには、さらに多くのことを行う必要があります。そのようなパターンを通じてブランチが観察される可能性があるため、コードの重要なセクションにブランチを含めないでください。  
 SGXも低速です。メモリ暗号化自体はオーバーヘッドをほとんど追加しませんが、コンテキストの切り替えはキラーです。  
SGXアプリのもう1つの例は、MicrosoftのCloud Key Vaultです。これにより、Azureテナントは、コードとは別にキー、パスワード、トークンなどのシークレットを保存できます[1309]。  
要するに、良いSGXコードを書くのは難しいです。  
 賢い人なら、信頼できるマルウェアを書くことができます。  
そして、あなたがインテルを完全に信頼しているとしても。 NSAがFISAの令状を使用してIntelにデバッグモードのエンクレーブを強制的に強制しないと信じている場合でも、MDKの侵害やサイドチャネルの悪用について心配していなくても、アプリのリスクは依然としてあります- HSMと同様に、層の露出。  
Intel（およびArm）は、エンクレーブテクノロジーの後続バージョンについて話しています。  
 マシンが盗まれたと報告された場合、キーを消去してCPUをブリックできます。  
 これは、Javatrusted実行環境を備えたさらに別のエンクレーブをサポートしており、開発者はそこで暗号を実行できます。たとえば、決済端末では、MEからPINパッドへのハードウェア信頼パスを設計できます[1698]。  
MEにも一連の脆弱性とエクスプロイトがありました。  
7。  
20。  
 2016–7年の間、暗号通貨はAIや量子と並んで、ビッグデータとモノのインターネットの後の誇大宣伝サイクルに置き換わりました。  
2008年、ビットコインは、中本聡の仮名を使用している誰かによって、ホワイトペーパーと実装を使用して静かにリリースされました[1375]。  
2011年2月、Ross Ulbrichtと呼ばれる若いリバータリアンが、政府の管理下にないオンライン市場であるSilk Roadを立ち上げました。  
 彼らはeBayのようにお互いを評価することができ、エスクローサービスがあり、購入者がビットコインを預けて商品の配送時にリリースできるようにしました。  
 他の地下市場もビットコインを採用しました。  
 さらなる取引需要は、為替管理で国からお金を引き出したい人々から来ており、金のような危機の時に購入される資産としてビットコインを見ている人々からの投資需要につながりました。  
ビットコインは複数の模倣者を生み出しました–それらのほとんどは詐欺ですが、いくつかの現実的な革新も。  
 これを書いている時点（2020年）では、熱狂のピークは過ぎましたが、暗号通貨は投資家にとって新しい資産クラスになり、金融規制当局や法執行機関に複数の問題を提起しています。ソフトウェアを書いている人々以外に信頼できる当事者はおらず、参加者の仮定された身元もありません。  
70〜$ 109。  
セキュリティエンジニアリング623ロスアンダーソン20。  
 ブロックチェーンセクション7。  
1。  
ここでは、基本的なメカニズムの概要を示します。  
 ビットコインブロックチェーンは、一連のトランザクションを含む追加専用ファイルです。  
 ユーザーはブロックチェーンにアドレスとして表示されます–公開鍵のハッシュである仮名。  
 ほとんどのトランザクションは、前のトランザクションから未使用のトランザクション出力（UTXO）を取得して1つ以上のアドレスに転送することにより、通貨をあるアドレスから別のアドレスに転送します。  
4。  
他のユーザーは、要求されたトランザクションのセットを自由に選択し、それらが有効であることを確認し、それらをブロックチェーンの新しいブロックにマイニングします。  
 トランザクションの各ブロックは、ブロックの内容のSHA256ハッシュとランダムなソルトによってマイナーによって認証されます。  
 このようなハッシュは作業の証明であり、テミスをランダムなプロセスで見つけるため、どの鉱山労働者が次の鉱山を見つけるかを予測することは困難です。  
パズルの難易度は、新しいブロックが約10分ごとに採掘されるように自動的に調整されます。  
 鉱山労働者は、自分が採掘したブロックごとにブロック報酬を受け取ります。執筆時点では、これは12です。  
7。  
 ユーザーは、取引の優先順位を得るために取引手数料を入札します。彼らは通常数十セント​​ですが、混雑時には数十ドルに上昇する可能性があります。  
 競合する次の2つのブロックが採掘される場合、鉱山労働者が最長のチェーンを採掘するというルールによって競合が解決されます。  
 それでも、大部分の鉱山労働者は、さらに遠くまで到達したチェーンを構築することによって、歴史を書き直すことができました。いわゆるチェーン再編成です。  
 ただし、ビットコインの総供給を制限するために、報酬は時々半分になり、報酬は6に低下する予定です。  
 したがって、マイニングリグに投資する人々は、ビットコインの価格が上昇し、規制当局が需要の抑制に影響を及ぼさないように賭けています。  
7。  
 競合が解決されない場合、結果として分岐が発生する可能性があります。システムは互換性のない2つの後続ノードを作成します。  
 しかし、いくつかのフォークは慎重に行われており、その起業家に加えて、数千のビットコインクローンが開始されました。そのほとんどは詐欺でした。  
 トランザクションには、支払いをプログラム可能にするスクリプトを含めることもできます。  
最初の2つは、プリンストンコンピュータサイエンティストのグループによる技術解説です。2015年には、Joe Bonneau、AndrewMiller、Jeremy Clark、Arvind Narayanan、Joshua Kroll、Ed Felten [293]による18ページの知識体系化論文があり、308ページあります。 Arvind Narayanan、Joe Bonneau、Ed Felten、Andrew Miller、Steven Goldfederによる本[1383]。  
 執筆時点では、これらは古くなっているので、以下では、その後の開発に集中します。  
暗号通貨で何がうまくいかないのかを理解するには、暗号数学だけでなく、もっと多くのことを検討する必要があります。  
20。  
1ウォレット当初、すべてのビットコインユーザーは仲間でした：完全なクライアントソフトウェアはビットコインを採掘し、採掘したコインを使うことができます。  
 1つ以上のUTXOのロックを解除する秘密鍵を知ってビットコインを所有しているため、アカウントに固有の概念はありません。  
 ウォレットのセキュリティは急速に大きな問題になりました。  
署名キーをハードディスクに保持し、パスフレーズで保護するソフトウェアウォレットは改善されていますが、マルウェアやその他の攻撃に対して脆弱です。  
 それでも、数百万ドル相当のビットコインを所有していることが知られている人々が、自宅で武装強盗に強奪され、譲渡することを余儀なくされていることは明らかです。  
 2013年までに、エクスチェンジまたは他のオンラインサービスプロバイダーがすべてを代行するホステッドウォレットの出現が見られました。  
7。  
 しかし、以下で説明するように、ホストされたウォレットは、他の広範な詐欺や悪用を引き起こしています。  
7。  
マイニングリグは、FPGAを使用して登場し、その後、汎用マシン上のソフトウェアよりもはるかに高速で実行されるASICを使用して登場しました。  
 2019年の暗号通貨採掘の総エネルギー消費量は約75TWhで、CO2排出量は3,500万トンを超え、ニュージーランドの二酸化炭素排出量に匹敵しました。鉱山労働者は自分たちの収入を平均化する少数の鉱山プールに組織化しました。  
 容量は貸し出すことができ、いわゆる51％攻撃で暗号通貨を攻撃するために使用されることがあります。  
 初期の頃、人々はそのような攻撃は即座に通貨の信頼性にとって致命的であると考えていましたが、現実はより複雑であることが判明しました。  
 しかし、その市場価値には大きな影響はありませんでした。  
 2020年8月にはさらに2つの攻撃があり、そのうちの1つは攻撃者が$ 5を盗むために必要なハッシュパワーを購入するために$ 192,000を費やしました。  
 したがって、ブロックチェーンを推論するときは、ゲーム理論と暗号について慎重に検討する必要があります。単純化した議論は常に現実と一致するとは限らない。  
7。  
 イーサリアムは、複雑なトランザクションを自動的に実行できるスマートコントラクトの見通しを保持しているため、時価総額による2番目の暗号通貨になります。  
 このような分散型の自律組織のアイデアは、バブル期に大きく宣伝されました。  
 2020年の時点で、主なアプリケーションは、分散取引所セキュリティエンジニアリング626ロスアンダーソン20の取引に関連しているようです。  
 BLOCKCHAINS（DEX）を使用すると、人の介入なしに、ある暗号通貨を別の暗号通貨と交換できます。  
）これは興味深い新しい故障モードにつながりました。  
現在、DEXの非効率性を取引の前倒し（予測と利用）によって悪用する裁定取引ボットが登場しています。  
 ボットのマイティン理論は市場のガバナンスを引き継ぎ、十分な資金を調達できればそれを略奪する[869]。彼らはすでにスマートコントラクトのバグを利用して大きな利益を上げています[1507]。  
2016年に、DAOと呼ばれる投資ファンドがイーサリアムブロックチェーンのスマートコントラクトとして設立され、1万人以上の投資家から1億5000万ドル以上を集めました。  
 これにより、元の暗号通貨取得ユニットの所有者が変更された通貨と「イーサリアムクラシック」の両方で、変更されていないバージョンが知られるようになったため、ブロックチェーンのハードフォークが生まれました。  
 病気の子供たちの世話をするために仕事に時間を費やさなければならない親にトペイを使用するという提案があり、それは店員がしばしば見逃す複雑な法的規則を持ち、上訴につながる。  
 しかし、インサイダー、ハッカー、ミスについてはどうでしょうか？地方自治体はハッキングされ、ランサムウェアを支払う傾向があります。  
 しかし、本当の契約違反者は、プロセスの制御を失うことに対する地方政府の恐怖でした。  
3。  
2。  
7。  
これは、身代金の支払いや麻薬のオンライン購入には十分な速度ですが、EMVと比べると印象的ではありません。  
7。  
人々は、レイヤー2プロトコルの例であるサイドチェーンを使用してこれを修正しようとしています。このようなプロトコルは、ビットコインやEthereumなどのレイヤー1プロトコルの外部でトランザクションを行います。  
重要なアイデアは、2つの条件付き転送で構成されるハッシュ化されたタイムロックコントラクト（HTLC）を使用して、暗号通貨を相互にコミットすることです。  
ボブも同様の取り組みを行っています。  
これを機能する支払いシステムに変えるには、かなり多くのエンジニアリングが必要です。  
 次に、アリスがボブ経由でチャーリーに支払うメカニズムとルーティングアルゴリズムを構築して、誰にでもお金を稼ぐことができます。  
 プロトコルのセキュリティには、他のユーザーが共謀したとしても、正直ユーザーがお金を失うことがないようにすることが含まれます。  
 2020年の主要なそのようなシステムはLightningネットワークです。これは、最終的な決済まで数秒で完了し、適切な電話アプリを持つ人々がWeChat Payと同じようにQRコードに支払うことができ、現在1日あたり1000件のトランザクションを処理しています。  
 そのため、悪意のあるユーザーは何百もの支払いを設定し、それらを数時間放置した後、無料でキャンセルできます。  
 規制当局が転送ノードを取り締まる可能性も非常に高いようです。  
7。  
 ほとんどが破産しました。多くの場合、彼らはハッキングされたため、またはインサイダーがお金を盗んでハッキングされたと主張したためです。  
裁判は継続します。当時のニュース報道では、内部統制とソフトウェア開発プロセスは無秩序だったと報告されています[1280]。  
 マウントゴックスのイノベーションの1つは、2013年の間に保管管理の交換になることでした。  
7。  
 それにより、19世紀の金融が金商人から銀行へと移行しました。保管庫に金貨の特定のバッグを所有するのではなく、顧客は今や銀行全体の資産に対する申し立てをしました。マウントゴックスの崩壊後の分析により、これらのトランザクションの多くはブロックチェーンに表示されていなかったことが明らかになりました。  
 （そして、それが今日までにいくつの交換が働いているかです。  
 2010–13年に交換が存在した最初の3年間でさえ、40の交換のうち18が崩壊した[1339]。  
 これに加えて、麻薬やその他の違法な商品が売買される地下市場の売上高は6億ドルで、2017年の値の約2倍です[400]。  
 ジョングリンとアミンシャムスは、ビットコインの価格がテザー（Uにペグされたデジタル通貨）を含むインサイダー取引によってサポートされていたことの証拠を提示します。  
 ドル、2017年のブームの間に[822]、多くの暗号通貨の市場価格がしばしば違法な操作の結果である可能性があるという見通しを高めました。  
市場操作はさておき、これまでで最大の単一の暗号通貨詐欺は、PlusTokenと呼ばれるPonziスキームであったように見えます。これは、主催者が2019年に逮捕される前に中国国民から30億ドルを獲得したものです[864]。  
 ランサムウェアは、2001年から2015年の間に、年間約200万〜300万ドルから年間800万ドルに増えました。この犯罪の種類は着実に増えていますが、身代金はギフトカード経由でも収集されます[1190]。  
 その年、世界最大のダークネット児童ポルノウェブサイトWelcome to Videoは、オペレーターがブロックチェーン上のビットコインのフローを介して追跡された後、閉鎖されたため、暗号通貨の偽名の性質には限界があります[551]。  
 定期的な交換はまた、法執行機関にとって生活を困難にします。  
ただし、ビットコインは仮名を使用しますが、ブロックチェーンにはすべてのトランザクションの永続的な記録が含まれています。  
 実際のトランザクションとデータにはコンテキストがあり、セキュリティエンジニアリング629ロスアンダーソン20を許可します。  
 BLOCKCHAINSinferencesが行われます。  
 ただし、これを行うと、マネーロンダリングの試みによってビットコインが汚染されます。合計で、ビットコインの10％が少なくとも1回盗まれたか、マネーロンダリングサービスを通過したと考えられます。  
例として、オハイオ州の男性は、3億ドルを洗浄したそのようなミキサーだけを操作したとして2020年に起訴された[553]。  
 現在、Moneroは最強のプライバシーを提供し、ソフトウェアを使用してコインを採掘できるように設計されています。そのコインの4％以上が他人のマシンで実行されているマルウェアによって採掘されています[1529]。  
 米国財務省の金融犯罪執行ネットワーク（FinCEN）は、マネーロンダリング防止（AML）と顧客情報（KYC）規制を世界中で推進しており、たとえばEUの第5のマネーロンダリング防止法などを通じて現地の法律に組み込まれています指令。  
 たとえば、ドイツの規制当局であるBaFinは、既存の金融規制を利用して、すべての取引所がライセンスを取得するように要求しています。 localbitcoinsとして。  
 しかし、執筆時点で最大のプッシュは、2019年のFinCENアドバイザリによるもので、10,000ドルを超えるトランザクションを処理する誰もが送信者と受信者の両方を特定し、疑わしい活動レポートを提出する必要がある「旅行ルール」を実装するために暗号通貨の交換が必要でした該当する場合。  
ヨーロッパでもさらなる規制が議題になっています。  
 あるイギリス人またはアメリカ人のユーザーがビットコインを別のユーザーに送金すると、トランザクションがブロックチェーンの近くに移動しない可能性がかなり高くなります。両方がコインベースの顧客である場合、コインベースはビットコインウォレットのウェブページに表示される残高を簡単に調整できます。  
EUでは、電子マネー指令が適用される可能性がありますが、英国とドイツの規制当局は、顧客が取引所と持っている従来の通貨残高に関してのみそれを施行します;取引所は、取引需要は投資需要よりもはるかに少ないため、仮想通貨は、支払いメカニズムとしてではなく、資産として扱う必要があります。  
 たとえば、銀行がセキュリティエンジニアリング630ロスアンダーソン20へのSIMスワップ攻撃をブロックする方法に多くの関心を示していることは注目に値します。  
 顧客の電話が失敗した暗号の夢、ほとんどの暗号通貨取引所はまったく関心を示していません–交換クレデンシャルはSIMスワップギャングの主なターゲットの1つであるという事実にもかかわらずです[1449]。  
20。  
6許可されたブロックチェーン暗号通貨とブロックチェーンを巡る誇大宣伝は商業的関心を呼び起こし、2015年頃からダボスから戻ってきたCEOはIT部門にブロックチェーンが必要だと告げました。これにより、Hyper-ledgerやEnterprise Ethereum Allianceなどのイニシアチブが生まれ、企業のサポーターがさまざまなブロックチェーンツールと標準を開発しました。  
 それらの多くは、コンセンサスメカニズムの一部としてSGXを使用しています。たとえば、インテル独自の経過時間の証明（PoET）提案などです。  
アプリケーションの例として、JPモルガンは、参加銀行がブロックチェーンに住宅ローンを入力できるようにする2015年のシステムに取り組みました。そのスクリプト言語により、トレーダーは、arbi-traryの複雑さの先物とオプションを作成できます。  
 1つの結論は、大多数のアプリケーションでは、ブロックチェーンは必要ないということです。前方に安全な封印されたログで十分です。  
 何よりも、ブロックチェーンアプリはレガシーシステムと通信する必要があり、アプリケーションのセキュリティミスやユーザビリティの危険を生み出す可能性が高くなることはありません。  
 そのような現実の経験は、バブルの最初の活気をなだめているように見えます。  
これは、金融、技術、その他の企業のコンソーシアムによって運営されることになっていたが、中央銀行からの大きな反対に遭い、その結果、Visa、MasterCard、PayPalなどの主要金融機関が撤退した。  
8失敗した暗号の夢多くの人々がブロックチェーンに基づく電子投票システムを提案しています。なぜなら、それらは不変であり、暗号を使用してそれらに機能を構築できるからです。  
9。  
 実際、2017年から8月のビットコインブームの間、一般的な学生プロジェクトの提案は「選挙をブロックチェーンに置くことで世界の平和を解決する」でした。  
 2018年、モスクワ市の3つの区のシステムは投票にイーサリアムブロックチェーンを使用しましたが、投票直前の2つの暗号化の脆弱性が修正されたため、投票の集計とブロックチェーン間のリンクが壊れ、ブロックチェーンが直後に消えました[782]。  
 MichaelSpecter、James Koppel、およびMITのDanny Weitznerは、リバースエンジニアリングを行い、攻撃とは無関係であったブロックチェーンのアプリの使用にもかかわらず、攻撃者が投票を公開または変更できる多数の脆弱性を発見しました[1810]。  
ブロックチェーンが選挙の問題を解決できるという考えは、経験豊富なセキュリティエンジニアを絶望させます。  
 権力のある締約国は、投票者の登録からキャンペーンの資金調達、広告ルールによるme-diaの検閲、投票者の脅迫、操作可能な投票スキームまで、スタックのすべてのレベルで規則を絶えず変更し、テクノロジーを覆しています。  
5。  
9要約1980年代に始まって、多くの人々が暗号をシステムセキュリティのある側面の信頼できるプラットフォームとして使用しようとしました。  
 その後、多くの暗号研究者（私を含む）は、暗号を使用して他のエコノミックおよび社会問題を解決できることを期待し始めました。  
 当時のCryptoおよびEurocrypt会議での研究論文は、このようなアイデアで溢れています。  
私たちのケーススタディは、技術的なポイント、経済的なポイント、およびポリシーのポイントを教えます。  
 FDEのような最も単純なアプリケーションでさえ、製品として成熟するにつれて複雑になり、実装の品質は大きく異なります。  
 SGXは非常に複雑なプロセッサで実行されるため、Security Engineering632Ross Anderson20です。  
 概要これは複数のサイドチャネル攻撃に対して脆弱であり、Intelはそれらのいくつかを脅威モデル内にあるとさえ考えていません。有能な意欲のある対戦相手があなたと同じマシンでコードを実行できる場合、基本的にトーストです。  
 アプリケーションが必要なインセンティブを作成すると、合理的なマイナーが履歴を書き換えようとしないという基本的な仮定でさえ失敗し始めます。  
経済的なポイントは、私たちがこれまでに採用してきた高度な暗号化メカニズムにはかなりのコストがかかることです。  
 SGXにはメモリ制限があり、コンテキストスイッチングの実際のパフォーマンスオーバーヘッドがあります。  
 スマートコントラクトは巧妙な処理を実行できる場合がありますが、実際には、他のソフトウェアと比較してサイズと範囲が非常に制限されています。  
ポリシーポイントは、高度な暗号化メカニズムはすべて、責任を問われることです。  
 したがって、それらを展開するか、または維持するかの決定には、微妙な外部性が含まれる場合があります。  
 SGXは、クラウドコンピューティングサービスの顧客に、最も価値のある資産を不正なシステム管理者や諜報機関から保護することを保証する方法と見なされています。実際のシステムは戦略的な理由で構築されており、市場の力であれ、政治の力であれ、作成者に力を生み出す、または定着させることを意味する傾向があります。  
 それらのほとんどで使用されている作業証明メカニズムは、合理的な人々が受け入れられないと考える可能性のあるCO2排出を引き起こし、実務におけるそれらの使用は、あらゆる種類の犯罪に巻き込まれます。  
法律担当者が炭素税について考えること、またはブロックチェーンを使用してそれらが生成するCO2を説明する組織を要求することも合理的です。  
セキュリティエンジニアリング633ロスアンダーソン20。  
 概要研究の問題暗号化とシステムセキュリティの境界を越える分散化には深い問題があります。  
 エンドツーエンドの暗号化は、PGPの影響にもかかわらず、SMTP電子メールの上に階層化することはできませんでしたが、Signalのような新しいプラットフォームがフラットから強制されるのを待つ必要がありました。  
 元々のサイファーパンクの理想は、政府や銀行など他の支配的なプレーヤーの関与なしに、交換の手段と価値の蓄積を提供する完全に分散した支払いシステムでした。  
 Bitcoinユーザーの大多数は暗号通貨を保持するために保管取引所に依存しており、これらの取引所はほとんどの取引を行います– DEXは0です。  
受託証券取引所は、実質的に規制されていない銀行になっています。  
 Torではこれはコミュニティですが、暗号通貨の世界では利益を求めて競合する開発者チームがいます。  
一般に、スマートコントラクトの信頼性はどうですか？ APIのセキュリティ問題に対するコンピューターサイエンスのアプローチは、インターフェースが安全であることを証明するために、正式な方法のツールを適応させることです。  
 スマートコントラクトは同様の問題に直面しており、バグを修正したり、状況の変化に対応したりするのが困難なため、複雑になっています。  
 これは慎重なエンジニアリングにすぎませんが、そのような交換の「信頼できない」というイデオロギー的正当化に疑問を投げかけます。  
ビットコインの仕組みの詳細については、プリンストンブック[1383]またはJEPペーパー[274]を参照してください。盗まれたビットコインの追跡と暗号通貨規制の詳細については、[116]を参照してください。  
 2015年のメッセージングアプリの遊びの状況の調査（SignalがメッセージングとVOIPの以前のアプリから統合されたとき）は、[1917]にあります。