NUMERO 1 IN ITALIA SU ELETTRONICA EMBEDDED E SEMICONDUTTORI

Firmware 2.0

#20
Gen-Feb 2022

IoT - Blockchain Cryptocurrency

IN QUESTO NUMERO:

PROGETTO PER LA GESTIONE IOT DI UN SISTEMA BLOCKCHAIN

PROGETTO DI UN SISTEMA IOT PER L'ACQUISIZIONE DEL PREZZO CORRENTE DEI BITCOIN

LA CRIPTOVALUTA IOTA (DI ELEKTOR)

PROGETTO DI UN SISTEMA DI SICUREZZA IOT CON IL SENSORE PIR HC-SR501

E MOLTO ALTRO!

it.emcelettronica.com

Elettronica Open Source

PROFESSIONAL & MAKER ZONE

Firmware 2.0 EDITORIAL PLAN 2022

COSA LEGGERAI NEL 2022?

TOPICS	MAKERS ZONE	DATA DI PUBBLICAZIONE
IoT	Blockchain/Cryptocurrency	1 Febbraio
AI/ML	Big Data Analytics	1 Marzo
Mems/Sensors	Self Driving	1 Aprile
Wireless/RF	Low Energy Smart Projects	1 Maggio
IoT	Voice Bot/Chat Bot	1 Giugno
Robotics	Cloud Computing	1 Luglio
IIoT/Automation	Smart Monitoring	1 Settembre
LED/Optoelectronics	Wearable	1 Ottobre
Embedded Boards Design	Microcontrollers Projects	1 Novembre
IoT	Cyber Security	1 Dicembre

Un nuovo inizio, trend e prospettive dell'Elettronica

Cari lettori,
un nuovo anno è appena iniziato e il nostro ringraziamento va a tutti voi che seguite e mostrate il vostro interesse per i ***contenuti innovativi di Elettronica Open Source****, sia sul blog sia sulla rivista digitale Firmware 2.0. Il lavoro messo a punto da Elettronica Open Source in questi intensi 15 anni è stato finalizzato sull'obiettivo di rendere accessibile al maggior numero possibile di persone la conoscenza sul vastissimo mondo dell'elettronica embedded, dei microcontrollori e delle tecnologie innovative attraverso* ***articoli tecnici e progetti open source****, sia complessi sia più basici e quindi facilmente realizzabili anche da chi è alle prime armi. L'obiettivo di Elettronica Open Source è quello di rendere tutti voi lettori in grado di realizzare i vostri progetti e prototipi in modo semplice e intuitivo attraverso* ***hardware e software open source****, utilizzando componenti di facile reperibilità e dai costi contenuti. Possiamo dire con un pizzico di orgoglio di aver centrato l'obiettivo, con la consapevolezza che è necessario sempre porsi nell'ottica del miglioramento continuo grazie ai feedback della nostra Community, la più grande* ***Community italiana di elettronica per makers e professionisti****, nella quale tutti voi che ne fate parte potete condividere liberamente idee e progetti. Siete proprio voi lettori a fornirci preziosi feedback sulla base di quelle che sono le vostre necessità professionali, formative oppure hobbistiche, e di questo non possiamo fare altro che ringraziarvi. Il primo topic del Piano Editoriale 2022 è incentrato sull'****IoT****, la* ***tecnologia Blockchain*** *e le* ***criptovalute****, trend dei quali sentiremo parlare molto da qui ai prossimi anni. Il 2021 è stato un anno importante, ma anche un anno di transizione. In una fase caratterizzata da difficoltà a causa della pandemia da Covid19, a crescere è stata la domanda e l'utilizzo di dispositivi IoT per i contesti più disparati, dalle applicazioni wearable, particolarmente diffuse come conseguenza di un maggiore livello di attenzione per il benessere e la consapevolezza del proprio stato di salute, ai dispositivi per la smart home, i sensori per il monitoraggio ed il controllo di parametri ambientali, le molteplici applicazioni dell'elettronica smart che rendono la nostra vita più efficiente.* ***L'Internet of Things è ovunque*** *e il trend in crescita per i prossimi anni nel numero di dispositivi connessi alla rete Internet e monitorabili da remoto fa ben sperare per il lungo periodo. Il 2022 sarà anche l'anno della* ***Embedded World Exhibition & Conference****, che si terrà a Norimberga dal 21 al 23 giugno, dove verranno presentate le più importanti soluzioni di ricerca e sviluppo nell'ambito delle tecnologie emergenti, elettronica embedded, IoT, efficienza energetica dei dispositivi elettronici, microcontrollori, Intelligenza Artificiale, soluzioni di connettività,* ***nonostante le forniture di chip siano ancora notevolmente limitate****. Per il futuro ci aspettiamo di assistere ad una continua innovazione e ricerca nell'elettronica, al fine di aumentare la fruibilità dei sistemi embedded e delle tecnologie innovative pensate per essere sempre più open source, facilmente accessibili ed alla portata di tutti.*

Buona lettura!

Giordana Francesca Brescia

IoT Blockchain/Cryptocurrency

Founder&Editor
Emanuele Bonanni

CFO
Lidia Balica

Editorial Assistant
Maria Pisani

Maker in Chief
Giordana Francesca Brescia

Advertising & Marketing
Cristian Balica
cristian@contangosl.com

Graphic Designer
Marilde Mirra

Circulation
Users - 144.190
Social Network - 129.946

© Copyright
Tutti i diritti di riproduzione o di traduzione degli articoli pubblicati sono riservati. Manoscritti e disegni sono di proprietà di Contango SL.
E' vietata la riproduzione anche parziale degli articoli salvo espressa autorizzazione scritta dell'editore. I contenuti pubblicitari sono riportati senza responsabilità, a puro titolo informativo.

Trust Platform Design Suite

Velocizzazione dello Sviluppo della Sicurezza, dal Prototipo alla Produzione

Semplifica lo sviluppo delle tue soluzioni di sicurezza integrata con Trust Platform Design Suite (TPDS).

Realizzata per supportare la pluripremiata Trust Platform per la famiglia CryptoAuthentication™, ovvero la nostra soluzione scalabile e flessibile per l'on-boarding di elementi sicuri, questa nuova piattaforma software dedicata semplifica lo sviluppo della sicurezza fornendo casi d'uso predefiniti che soddisfano i più diffusi requisiti di mercato.

Disponibile ora nella versione 2 (v2) di TPDS, la nostra ultima versione del software consente alle terze parti nostri partner di aggiungere anche i loro casi d'uso, ampliando così le già molto ampie possibilità offerte agli sviluppatori di implementare le migliori opzioni di sicurezza oggi disponibili. Tra gli altri miglioramenti troviamo il supporto per soluzioni di sicurezza aggiuntive come il TA100, il primo dispositivo crittografico complementare per il mercato automobilistico.

Caratteristiche salienti

- Il flusso di on-boarding completamente integrato è in grado di portarti in poche mosse dalla scelta della soluzione al provisioning sicuro
- Compatibile con i sistemi operativi Windows® e macOS®
- Disponibile al pubblico per il download con Trust&GO e TrustFLEX

TRUST FLEX

TRUST &GO

TRUST CUSTOM

MICROCHIP

microchip.com/v2TPDS

Il nome e logo Microchip e il logo Microchip sono marchi industriali registrati e CryptoAuthentication è un marchio industriale di Microchip Technology Incorporated negli U.S.A. e in altri Stati. Tutti gli altri marchi menzionati sono di proprietà dei rispettivi titolari. © 2022 Microchip Technology Inc. Tutti i diritti riservati.
DS00004331A. MEC2409A-ITA-01-22

PROGETTO PER LA GESTIONE IOT DI UN SISTEMA BLOCKCHAIN

di **Fulvio De Santis**

Questo articolo intende descrivere un progetto dimostrativo di approccio all'interazione con la tecnologia Blockchain mediante l'impiego di un dispositivo IoT a basso costo. Nello specifico, il progetto realizzerà l'interfacciamento della scheda di sviluppo ESP32 con la piattaforma Blockchain Algorand. Gli elementi chiave della specifica Algorand impostano le basi per creare soluzioni più avanzate mirate all'impiego di dispositivi con risorse limitate. Nel progetto verrà utilizzata come esempio una semplice applicazione per dimostrare come un dispositivo IoT a basso costo possa rispondere ai comandi inviati dagli utenti sulla piattaforma Blockchain.

INTRODUZIONE - BLOCKCHAIN

Chi Blockchain è un **registro digitale pubblico** a cui tutti hanno accesso senza che un'autorità centrale ne abbia il controllo. È una tecnologia che consente agli individui e aziende di interagire con fiducia e trasparenza nelle transazioni. Una delle più conosciute applicazioni blockchain sono le valute crittografiche come Bitcoin e altre, ma sono possibili molte altre applicazioni. La tecnologia blockchain è considerata la forza trainante della prossima rivoluzione tecnologica dell'informazione. Molte implementazioni della tecnologia blockchain sono attualmente ampiamente disponibili, ognuna con la particolare peculiarità per uno specifico dominio applicativo, una di queste è la **Blockchain Algorand**. A differenza di un'architettura centralizzata, che presenta diversi problemi tra cui il guasto in un singolo punto e problemi di scalabilità, la blockchain utilizza un registro decentralizzato e distribuito per impiegare le capacità di elaborazione di tutti gli utenti partecipanti alla rete blockchain, contribuendo a ridurre la latenza e ad eliminare guasti in un singolo punto. L'**Immutabilità** è una caratteristica essenziale della blockchain, ovvero la capacità di garantire l'integrità delle transazioni creando registri immutabili. Nelle architetture centralizzate tradizionali, i database possono essere modificati e la fiducia con una terza parte deve essere creata per garantire l'integrità delle informazioni.

Nella tecnologia blockchain, poiché ogni blocco nel registro distribuito si riferisce al blocco precedente che costituisce una catena di blocchi, i blocchi vengono salvati in modo permanente e non vengono mai modificati finché l'utente partecipante continua a mantenere la rete. La blockchain offre un alto livello di **Trasparenza** condividendo i dettagli della transazione tra tutti gli utenti partecipanti coinvolti in tali transazioni. In un ambiente blockchain non è necessario l'intervento di una terza parte, il che migliora la facilità d'uso e garantisce un flusso di lavoro affidabile. Sebbene la sicurezza rappresenti un problema per la maggior parte delle nuove tecnologie, la blockchain garantisce una sicurezza migliore perché utilizza un'infrastruttura a chiave pubblica che protegge da azioni dannose atte a modificare i dati. Gli utenti partecipanti della rete blockchain ripongono la loro fiducia nelle caratteristiche di integrità e sicurezza del meccanismo di consenso. Inoltre, la blockchain elimina il singolo punto di guasto, che colpirebbe l'intero sistema. L'**Efficienza** della blockchain migliora la classica architettura centralizzata distribuendo i record del database tra i vari utenti coinvolti nella rete blockchain. La distribuzione delle transazioni rende più trasparente la verifica di tutti i record archiviati nel database. Una blockchain è più efficiente della classica architettura centralizzata in termini di costi, velocità e gestione del rischio.

LA PIATTAFORMA ALGORAND

Algorand è una piattaforma di criptovaluta basata su blockchain, che ha l'obiettivo di garantire sicurezza, scalabilità e decentralizzazione. La piattaforma Algorand supporta la funzionalità **Smart Contract** (contratto intel-

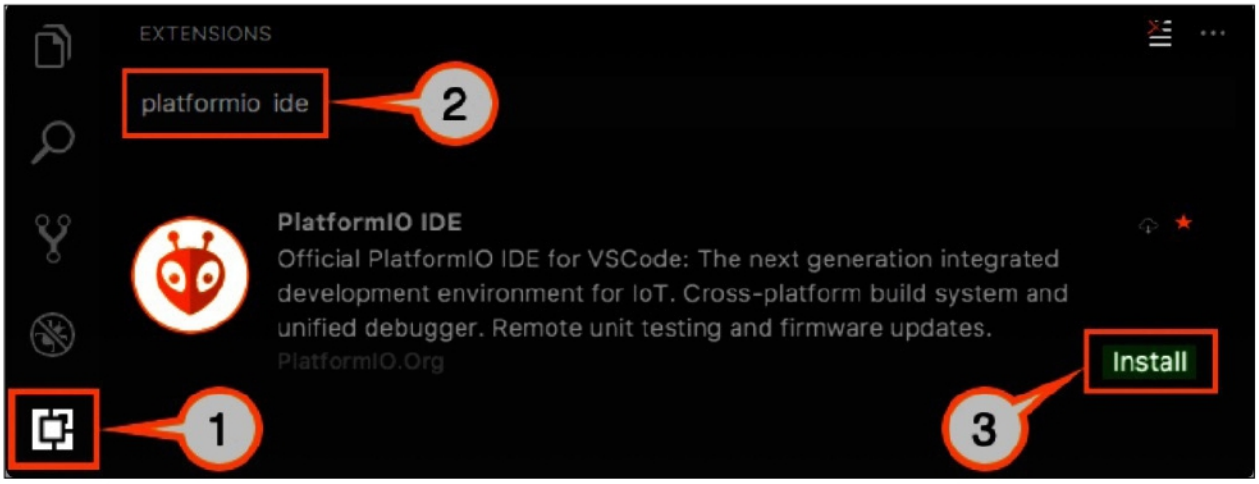


Figura 1: Installazione PlatformIO IDE

ligente) e il suo algoritmo di consenso si basa sui principi Proof of Stake (protocolli di una classe di funzionalità di consenso per blockchain, che operano selezionando i validatori in proporzione alla loro quantità di partecipazioni nella criptovaluta associata). La criptovaluta nativa di Algorand si chiama Algo.

Una libreria C/C++ di base supporta funzionalità come la generazione di chiavi **Ed25519** (Ed25519 è un sistema di firma a chiave pubblica), il recupero di informazioni sull'account e le transazioni.

IL PROGETTO

La finalità del progetto è di ottenere un **dispositivo IoT** (l'**ESP32**) in grado di connettersi a un AP Wi-Fi locale, creare il proprio account Algorand generando una coppia pubblica/privata di chiavi, salvare l'indirizzo (chiave pubblica) in una memoria non volatile per garantire la continuità delle attività dopo i riavvii, monitorare l'account per un evento finanziario, infine, monitorare il suo account per i viare e ricevere criptovaluta Algo e token, organizzare e tenere traccia di tutti i propri portafogli Algorand, gestire le proprie risorse e altro ancora. Nel progetto viene utilizzato per gestire l'account, TESTNET, che creeremo e per inviare i comandi al dispositivo IoT; **Algorand TestNet Dispenser** viene utilizzato per consentire lo sviluppo di test sulle reti blockchain di Algorand. In pratica, dispensa gli Algo (criptovaluta) che non hanno alcun valore monetario e vengono utilizzati solo per testare le applicazioni blockchain; **PureStake.io** è un servizio per l'accesso alla rete Algorand affidabile e sicuro e alle API REST native di Algorand per MainNet, TestNet e BetaNet. In questo progetto utilizzeremo un'API per interagire con TESTNET dal dispositivo IoT; **Algorand-esp32-example-master** è il codice di esempio che installeremo nell'ESP32. Sarà inoltre necessario creare un Punto di accesso Wi-Fi locale a cui collegheremo l'ESP32 consentendogli di interagire con la blockchain.

QUELLO CHE HAI LETTO E' UN ESTRATTO, L'ARTICOLO COMPLETO E' RISERVATO AGLI ABBONATI AD ELETTRONICA OPEN SOURCE.

PERCHE' ABBONARSI A PLATINUM 2.0?

UN ANNO DI FIRMWARE 2.0
TUTTI GLI ARTICOLI TECNICI RISERVATI
CONTEST E PROMOZIONI RISERVATI

VOGLIO ABBONARMI!

PROGETTO DI UN SISTEMA IOT PER L'ACQUISIZIONE DEL PREZZO CORRENTE DEI BITCOIN

di **Fulvio De Santis**

In questo articolo descriveremo il progetto di un sistema di acquisizione del prezzo corrente dei Bitcoin mediante il quale saremo in grado di conoscere in tempo reale il prezzo dei Bitcoin espresso in dollari americani (USD), sterline inglesi (GPB) e in valuta dell'Unione Europea (EURO). Nello specifico, viene utilizzato il modulo ESP-01 con chip ESP8266, un dispositivo IoT a basso costo impiegato come client HTTP tramite il quale viene richiesto e ottenuto dal web in tempo reale il prezzo dei Bitcoin.

INTRODUZIONE AI BITCOIN

Bitcoin è una **valuta digitale** sicura (criptovaluta) che **opera senza alcun controllo centrale** o supervisione di banche o governi. La sua applicazione si basa su software e crittografia peer-to-peer. Un **registro pubblico digitale** (**Blockchain**) registra tutte le transazioni Bitcoin le cui copie sono conservate nei server in tutto il mondo. Chiunque disponga di un computer può configurare uno di questi server, noti come nodi. Il consenso su chi possiede tali monete viene ottenuto crittograficamente attraverso questi nodi server piuttosto che fare affidamento su una fonte centrale di fiducia come una banca. Ogni transazione viene trasmessa pubblicamente alla rete e condivisa da nodo a nodo. Ad intervalli di tempo prestabiliti, queste transazioni vengono raccolte insieme in un gruppo chiamato "blocco" e aggiunte in modo permanente alla blockchain. Allo stesso modo in cui si tengono le monete tradizionali in un portafoglio fisico, le valute virtuali sono conservate in **portafogli digitali** accessibili mediante software client o da vari strumenti online e hardware. I Bitcoin attualmente possono essere suddivisi in sette cifre decimali: un millesimo di Bitcoin è noto come milli e un centomilionesimo di Bitcoin è noto come satoshi. In realtà, non esiste il Bitcoin o un portafoglio, in quanto è solo un accordo tra gli utenti della rete sulla proprietà di una moneta. Una chiave privata viene utilizzata per dimostrare alla rete la proprietà dei fondi quando si effettua una transazione. Una persona potrebbe semplicemente memorizzare la propria chiave privata e non aver bisogno di nient'altro per recuperare o spendere il proprio denaro virtuale, un concetto noto come "portafoglio della mente".

IL PREZZO DEL BITCOIN

Il Bitcoin ha una grande considerazione in tutto il mondo da parte di diversi organismi come investitori, ricercatori, commercianti e politici, per il pagamento digitale o semplicemente per scopi di investimento. L'obiettivo di questi organismi è di poter **gestire la volatilità del prezzo del Bitcoin** mediante metodologie di previsione e ottenere così un'elevata precisione del prezzo. Prevedere con precisione il prezzo del Bitcoin significa prendere in considerazione vari parametri che influenzano il valore del Bitcoin. In primo luogo, si punta a comprendere e identificare le tendenze quotidiane nel mercato dei Bitcoin, ottenendo al contempo informazioni sulle caratteristiche ottimali che circondano il prezzo di Bitcoin. Il set di dati può includere varie funzionalità relative al prezzo del Bitcoin e alla rete di pagamento. Utilizzando le informazioni disponibili, **è possibile predire il segno della variazione giornaliera del prezzo** con la massima precisione possibile. Nono-

stante il particolare interesse del pubblico, la comprensione teorica del valore di questa criptovaluta è limitata. Ecco perché la ricerca attuale sta cercando di trovare metodi validi per valutare il fenomeno complesso del **prezzo del Bitcoin**. La volatilità del suo prezzo presenta una certa specificità rispetto alle valute tradizionali. Per comprendere le ragioni di questa volatilità, è necessario identificare e analizzare le principali determinanti del prezzo del Bitcoin e stimarne l'influenza.

La grande fluttuazione del prezzo di Bitcoin è causata da molti fattori che possono essere suddivisi in due categorie. Innanzitutto, il mercato dei Bitcoin è un mercato di recente sviluppo. Non esiste una rappresentazione fisica legata a questo tipo di risorsa virtuale. Nel contempo, un gran numero di singoli investitori può essere facilmente colpito dalla manipolazione del mercato, inducendoli a prendere di conseguenza decisioni irragionevoli. Tutti questi problemi (notizie false, manipolazioni o altri motivi) portano a una grande fluttuazione del prezzo del Bitcoin. In secondo luogo, il mercato dei Bitcoin non è regolamentato dai governi. Mancano sostanzialmente i regolatori nei mercati finanziari tradizionali nel campo delle criptovalute. Ad esempio, le notizie false influenzano spesso le decisioni dei singoli investitori. Inoltre, Bitcoin è un prodotto globale che è interessato dalla regolamentazione in tutto il mondo. Ad esempio, la forte riduzione del prezzo di Bitcoin di quasi il 50% all'inizio del 2018 è stata causata principalmente dalle normative governative in Corea del Sud e Cina, che vietano le offerte iniziali di monete. Il grande problema delle **fluttuazioni del prezzo del Bitcoin** scaturisce nella necessità di realizzare una soluzione per la previsione della fluttuazione del prezzo di Bitcoin poiché molti investitori si preoccupano di più se avviene improvvisamente l'aumento o la caduta del prezzo del Bitcoin. Questo problema può essere semplicemente descritto dai pochi campioni. Inoltre, non conviene prendere in considerazione le informazioni basate sulle notizie poiché è difficile determinare l'autenticità di una notizia o prevedere il verificarsi di emergenze. Pertanto, vengono utilizzati solo i dati basati sul prezzo a livello di minuti. I dati basati sul prezzo possono anche rivelare alcuni comportamenti di manipolazione. Ad esempio, i manipolatori venderanno gradualmente le loro criptovalute quando i prezzi salgono. Altrimenti, se le vendono quando i prezzi scendono, i prezzi diminuiranno rapidamente. Quindi, i prezzi di negoziazione saranno piuttosto bassi per loro. I manipolatori acquisteranno gradualmente le loro criptovalute quando i prezzi scendono. Altrimenti, se li acquistano quando i prezzi salgono, questo comporterà per loro un costo di negoziazione elevato. Queste caratteristiche di base si riflettono sulle **variazioni del prezzo di Bitcoin**.

IL PROGETTO

Nel progetto viene utilizzato l'hardware **ESP-01** con **chip ESP8266**, il convertitore seriale UART-USB **CH340**, il software **NodeMCU** ed ESPlorer. Una volta programmato, il modulo ESP-01 opererà come client HTTP e, con opportuni comandi, sarà in grado di ricevere dal web il prezzo corrente dei Bitcoin.

PROGRAMMAZIONE DELL'ESP-01 CON NODEMCU

Per programmare l'ESP-01 utilizzeremo **NodeMCU**. NodeMCU è un **firmware** per programmare dispositivi NodeMCU DEVKIT ed è possibile utilizzarlo anche per programmare le **schede ESP8266** con script **LUA**. LUA è un linguaggio di programmazione potente e veloce. Facile da imparare e utilizzare, può essere integrato nelle applicazioni, come nel caso di questo progetto. NodeMCU è un **tool** di programmazione simile ad Arduino ma più

QUELLO CHE HAI LETTO E' UN ESTRATTO, L'ARTICOLO COMPLETO E' RISERVATO AGLI ABBONATI AD ELETTRONICA OPEN SOURCE.

PERCHE' ABBONARSI A PLATINUM 2.0?

UN ANNO DI FIRMWARE 2.0
TUTTI GLI ARTICOLI TECNICI RISERVATI
CONTEST E PROMOZIONI RISERVATI

VOGLIO ABBONARMI!

LA CRIPTOVALUTA IOTA (ED UN FPGA PER L'RPI) – PARTE 1: MACCHINE CHE PAGANO MACCHINE

Grazie al progresso tecnologico, i device appartenenti all'ecosistema dell'Internet of Things (IoT) diventano sempre più piccoli e compatti, economici ed efficienti in termini di consumi energetici. Questi dispositivi implicano la generazione di un flusso di dati che deve essere in qualche modo gestito. Una potenziale soluzione è quella di fornire strumenti flessibili online capaci di elaborare questi dati, e il cui pagamento verrebbe gestito automaticamente dai nodi IoT. In un contesto del genere ecco che entra in gioco una criptovaluta come IOTA. In questa prima parte dell'articolo ne descriviamo gli aspetti fondamentali, mentre nella prossima presenteremo una scheda d'estensione HAT basata su un FPGA per Raspberry Pi, in grado di accelerare le transazioni IOTA.

INTRODUZIONE

Il potenziale campo di applicabilità del mondo IoT è molto ampio e variegato. Un frigorifero in grado di programmare la spesa automaticamente, un'automobile che stabilisce l'itinerario in maniera indipendente con l'ausilio di dati sul traffico in tempo reale, oppure ancora una lavatrice in grado di avvisarci tramite notifica su smartphone quando termina il ciclo di lavaggio; questi sono solo alcuni degli esempi più ovvi che possiamo citare. Non ci sono limiti all'immaginazione.

Molti device IoT sono dedicati esclusivamente all'acquisizione di dati. Per esempio, un'ampia gamma di sensori rileva dati meteorologici utilizzabili per un'accurata analisi globale sul clima, altri sensori sono dedicati alla raccolta di dati sulle radiazioni per permettere di conseguenza di realizzare una mappa del livello radioattivo attuale del Giappone, e ancora altri integrati nelle smart home come contatori elettrici, al fine di misurare il consumo energetico e il profilo di utilizzo. Questo permette ai fornitori di energia elettrica di **migliorare le previsioni dei picchi di carico e, di conseguenza, ottimizzare l'infrastruttura di rete**.

Ma l'Internet of Things va oltre tutto ciò. Ci indirizza verso un'**economia delle macchine**, dove queste ultime possono pagare i servizi resi disponibili da altre macchine. La compagnia di ricerca di mercato Gartner nel 2017 [1] pronosticò che nel 2020 il **numero di dispositivi connessi ad Internet** sarebbe stato di circa **20 miliardi**. La grande diffusione di dispositivi IoT implica però anche una **mole di dati sempre più vasta**, che potrebbe travolgere la tecnologia attuale in un futuro prossimo. La prima domanda è: dove mettere tutti questi dati? E se si trova un'adeguata posizione per l'archiviazione dei dati, come accedervi e come utilizzarla? È proprio qui che entra in gioco **IOTA**. IOTA ha la funzione di risolvere tutte le difficoltà tecniche, sia presenti che future, relative alla crescente popolarità e diffusione dell'IoT.

QUALI SONO LE PROBLEMATICHE CHE CONSENTE DI RISOLVERE IOTA?

Lo sviluppo delle criptovalute come Bitcoin ed Ethereum ci ha fornito registri virtuali decentralizzati, a prova di manomissione e altamente sicuri, che tutti possono utilizzare in modo anonimo e senza permesso esplicito, grazie all'ausilio delle **chiavi crittografiche user-generated**. La visione è stata estasiante sin dall'inizio, quando è diventato improvvisamente possibile trasferire denaro virtuale peer-to-peer senza intermediario e senza doversi affidare ad un'autorità centrale. Sfortunatamente, qualche difetto di progettazione non previsto si è rivelato nel tempo: i siste-

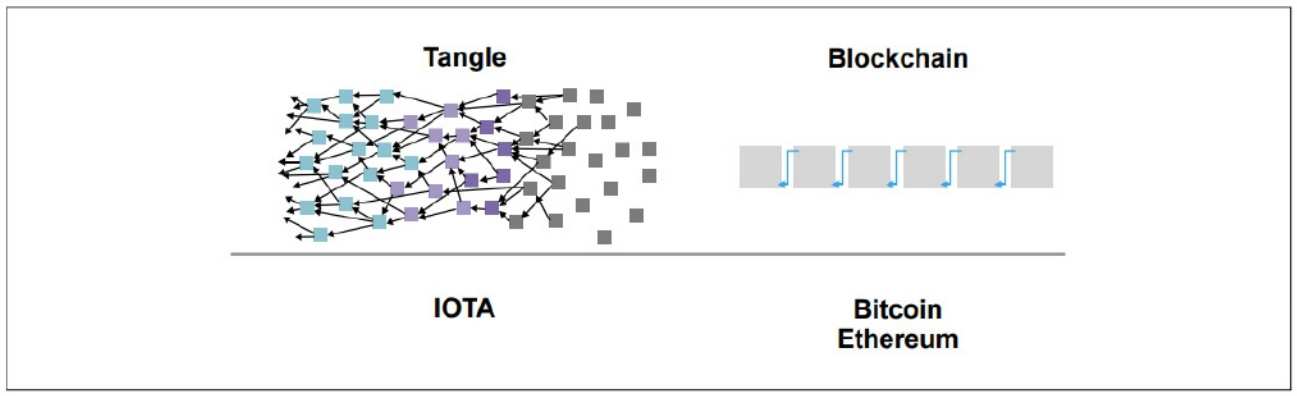


Figure 1. A directed acyclic graph versus a blockchain [8].

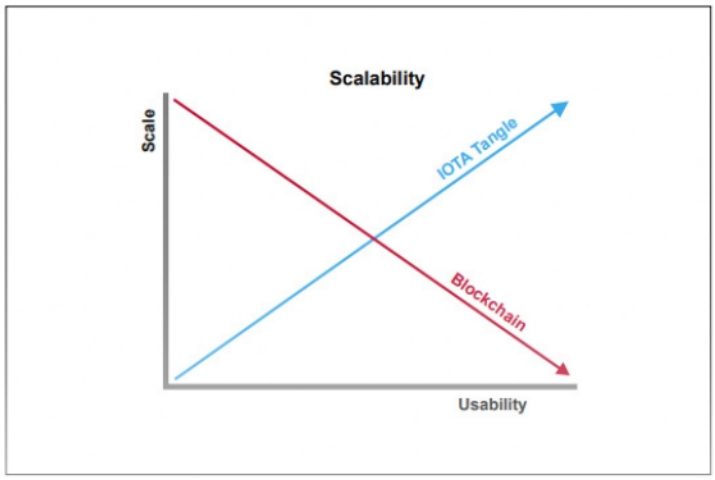


Figure 2. The IOTA tangle is vastly superior to a blockchain in terms of scalability [9].

rete di transazioni popolata di dati viene chiamata **tangle**.

I vantaggi sono evidentemente chiari: le blockchain presentano problemi di scalabilità, mentre i tangle IOTA non presentano difetti o colli di bottiglia che limitano la velocità massima di transazione. Di fatto, le performance del tangle aumentano in maniera proporzionale con l'aumento del numero di transazioni effettuate (**Figura 2**).

Oltre al trasferimento di criptomoneta, IOTA abilita le transazioni "senza valore", il che significa che il tangle può essere utilizzato come infrastruttura di archiviazione per tutti i tipi di pacchetti di dati. Ideale per quel tipo di dati ottenuti dai sensori, per esempio, e senza che alcuna commissione venga addebitata per le transazioni.

mi blockchain di prima generazione (Bitcoin) e di seconda generazione (Ethereum con Smart Contract), infatti, si

Inoltre, ci sono estensioni ufficiali del protocollo per massimizzare il livello di funzionalità, come MAM (Masked Au-

QUELLO CHE HAI LETTO E' UN ESTRATTO, L'ARTICOLO COMPLETO E' RISERVATO AGLI ABBONATI AD ELETTRONICA OPEN SOURCE.

PERCHE' ABBONARSI A PLATINUM 2.0?

UN ANNO DI FIRMWARE 2.0
TUTTI GLI ARTICOLI TECNICI RISERVATI
CONTEST E PROMOZIONI RISERVATI

VOGLIO ABBONARMI!

LA CRIPTOVALUTA IOTA (ED UN FPGA PER L'RPI) – PARTE 2: PIDIVER – UNA SCHEDA FPGA PER CALCOLI RAPIDI

Nella parte precedente dell'articolo "La criptovaluta IOTA (ed un FPGA per l'RPi)" vi abbiamo presentato IOTA, la criptovaluta che permette ai nodi IoT di pagare gli altri utenti iscritti, ad esempio per l'archiviazione dei dati [1]. Al fine di eseguire le transazioni IOTA, prima di tutto bisogna risolvere il task di calcolo proof of work; questo protocollo serve a proteggere il database (tangle) dallo spam. Anche i computer x86 fanno fatica ad eseguire questo task aritmetico, ma IOTA consente ai piccoli nodi IoT di delegare il lavoro a device esterni specializzati. La seconda parte dell'articolo introduce la piattaforma basata su una scheda add-on FPGA per il Raspberry Pi.

INTRODUZIONE

Questa sezione dell'articolo descrive una soluzione rapida ed efficiente in termini energetici per la problematica inerente al PoW (Proof of Work) di IOTA; i calcoli necessari vengono eseguiti da un **FPGA**. Questo raggiunge un tempo medio PoW di 300 ms, che non solo risulta più veloce della libreria multithread ottimizzata SSE su Core i5 (circa 1.7 s), il consumo energetico di 2 Watt è anche significativamente diminuito.

PROOF OF WORK DI IOTA

Per fare in modo che una transazione venga accettata dal tangle, gli ultimi 14 step [1] dell'hash della transazione devono corrispondere a zero. Se un hash non rispetta questa condizione, un counter (vedere **Figura 1**) viene incrementato nella transazione e l'hash di quest'ultima viene ricalcolato. Questo processo viene ripetuto finché non si trova un hash valido. In media, per risolvere questo problema di calcolo sono necessari 314/ hps secondi, considerando che hps corrisponde al numero di funzioni hash che possono essere calcolate al secondo. Questo risulta in una media di 4.78 milioni di interazioni eseguite prima che il problema venga risolto.

L'idea di fondo è che il tangle può essere protetto dallo spam, dato che **la velocità massima di transazione raggiungibile viene nettamente ridotta dallo sforzo computazionale**. La fase di verifica invece richiede una insignificante quantità di tempo, poiché l'unica cosa da controllare è l'**hash della transazione**. Un hash di transazione valido viene dunque definito **proof of work** perché consiste nella prova verificata della correttezza del calcolo eseguito.

L'algoritmo di hashing CURL-P81 utilizzato -simile a SHA3- è progettato in costruzione di spugna. Nuovi blocchi con una dimensione (velocità) fissa, vengono assorbiti nello stato interno, il quale si caratterizza per dimensioni (e capacità) 3 volte maggiori a quelle di un blocco singolo. L'intero stato viene poi convertito nello stato successivo utilizzando una funzione spugna (**Figura 2**). Una volta che tutti i blocchi sono stati assorbiti, l'hash può essere esternato. Una transazione IOTA consiste in 33 blocchi, di cui ognuno contenente 81 trits (B1-B33 nel diagramma). L'ultimo blocco contiene il counter, che viene incrementato se l'hash della transazione non soddisfa le condizioni della

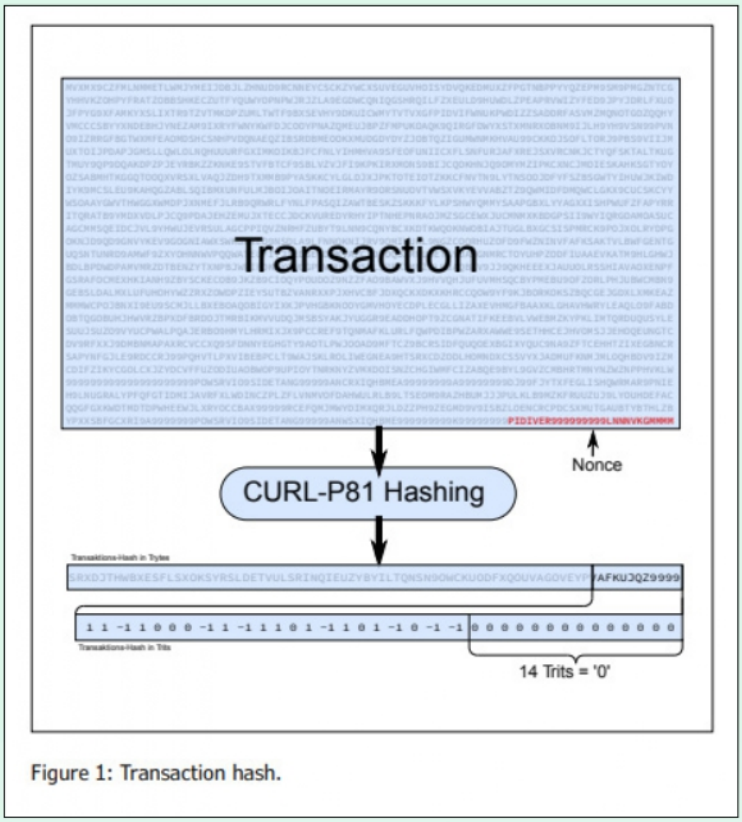


Figure 1: Transaction hash.

rete principale (ci sono altre reti tangle per sviluppo e test). Dal momento che il counter si trova solo nell'ultimo dei 33 blocchi, lo stato successivo all'assorbimento del 32esimo blocco (stato intermedio) può essere utilizzato come stato iniziale per il 33esimo blocco. Dopo aver incrementato il counter dell'ultimo blocco, è necessario attribuire un hash a un singolo blocco, al fine di calcolare l'hash dell'intera transazione; ciò permette di risparmiare molto tempo.

UNA PANORAMICA SUL PIDIVER

Il PiDiver - il nome deriva dall'unione della parola **Raspberry Pi** e dell'**algoritmo PoW "Pearl-Diver"** [1] - è un HAT (**Hardware Attached on Top**) per Raspberry Pi, capace di **eseguire i calcoli di proof of work di IOTA** in maniera celere ed efficiente in termini energetici. La **Figura 3** mostra la connessione del blocco del PiDiver. Al centro si trova un **FPGA** Cyclone 10 LP di Intel. Si tratta di un membro relativamente nuovo della famiglia Cyclone (pubblicato nel 2018) e progettato da Intel per soddisfare in particolare quel target di applicazioni IoT caratterizzate da un basso costo e da un consumo energetico ridotto.

Gli FPGA, che offrono molte **risorse logiche**, sono interessanti non solo perché hanno un basso costo e un'alta efficienza energetica, ma anche perché è possibile trovarne molte varianti sul mercato, con alloggiamenti differenti DIY e relativamente "friendly" (EQFP), e ciò li rende perfetti per questo progetto. L'FPGA è regolato a **200 MHz** e può calcolare un giro completo di hashing a ogni ciclo di orologio (CURL-P81 utilizza 81 giri). Inoltre, può calcolare sette funzioni di hash con counter differenti (non-cents) in modo simultaneo. Oltre agli 81 cicli, sono richiesti altri due cicli per il controllo del risultato, il ripristino dello stato precedente (stato intermedio in **Figura 2**) e l'impostazione dei valori del nuovo counter. Si ottiene circa 16.8 MHash/s. Nel caso della rete principale IOTA, il tempo medio per la fase PoW corrisponde approssimativamente a 300 ms o 3.33 PoW/s, trasferimento dati incluso. Inoltre, vi è un **microcontroller STM32** (STM32F302) nel circuito, che consente di operare l'FPGA tramite USB. Il proof of work può così essere eseguito sia attraverso l'interfaccia SPI di Raspberry Pi, sia su PC tramite USB (senza Raspberry Pi). Avrai notato che non c'è memoria flash per la

QUELLO CHE HAI LETTO E' UN ESTRATTO, L'ARTICOLO COMPLETO E' RISERVATO AGLI ABBONATI AD ELETTRONICA OPEN SOURCE.

PERCHE' ABBONARSI A PLATINUM 2.0?

UN ANNO DI FIRMWARE 2.0
TUTTI GLI ARTICOLI TECNICI RISERVATI
CONTEST E PROMOZIONI RISERVATI

VOGLIO ABBONARMI!

PROGETTO DI UN SISTEMA DI SICUREZZA IOT CON IL SENSORE PIR HC-SR501 – PARTE 1

di **Fulvio De Santis**

In questo articolo descriveremo la prima parte del progetto IoT di un sistema di sicurezza basato sul sensore di movimento PIR HC-SR501 e il modulo Wi-Fi ESP-01. Questo sistema di sicurezza è in grado di attivare un messaggio audio di segnalazione di intrusione mediante il modulo vocale ISD1820 e, nel contempo, di inviare un'e-mail quando il sistema rileva la presenza di una persona o di un animale. Inoltre, grazie all'impiego del modulo Wi-Fi ESP-01, il sistema di sicurezza può essere attivato/disattivato da remoto via internet da qualsiasi parte del mondo. Con il modulo vocale ISD1820 è possibile registrare una traccia audio di 10 secondi che viene riprodotta su comando del sensore PIR. L'e-mail di allarme intrusione viene inviata con data e ora dell'evento ad un predefinito indirizzo email.

DESCRIZIONE DEL PROGETTO

In **Figura 1** è riportato lo schema elettrico del sistema di sicurezza IoT.

Il circuito è alimentato da due regolatori di tensione, il regolatore LM1084-3V3 da 3,3 V che alimenta l'**ESP8266** e il transistor Q2, e il regolatore 7805 da 5 V che alimenta il **sensore PIR HC-SR501** e il **modulo vocale ISD1820**. Entrambi i regolatori sono alimentati tramite un adattatore da 12 V in corrente continua o da una batteria da 9 V essendo molto basso il consumo di energia di questo circuito. Il sensore PIR e il modulo vocale si attivano mediante un livello alto applicato dal pin GPIO2 dell'ESP-01, attraverso il resistore R1 da 1k di limitazione della corrente, alla base del transistor Q1 BC547 che, andando in conduzione, porta a massa i pin GND dei due moduli chiudendo così il circuito di alimentazione per entrambi.

L'impiego del transistor Q1 è stato necessario in quanto la corrente erogabile dal pin GPIO2 è insufficiente per alimentare i due moduli. Il pin GPIO0 viene utilizzato per programmare l'ESP8266 e come ingresso digitale del segnale proveniente dal pin OUT del sensore PIR tramite il transistor Q2 BC547 e il resistore R2 da 1k. Quando il pin GPIO va a livello alto, una funzione del software attiva l'invio di un'e-mail per segnalare l'avvenuta intrusione. Inoltre, in generale, i pin GPIO dell'ESP8266 non devono essere caricati (non assorbire/erogare eccessiva corrente) durante l'accensione, altrimenti il modulo ESP avvierà un ciclo di reset continuo. Per evitare ciò, sono stati previsti due interruttori per scollegare i pin GPIO temporaneamente durante l'accensione. Riguardo gli switch SW1, SW2 e SW3, lo switch SW3 sarà utilizzato nella fase di **programmazione dell'ESP8266** che tratteremo nella seconda parte del progetto in un successivo articolo in cui spiegheremo la funzione anche degli altri due switch SW1 e SW2.

I COMPONENTI PRINCIPALI DEL PROGETTO

I componenti fondamentali del progetto sono tre: il modulo Wi-Fi ESP-01 che integra il chip ESP8266, il sensore PIR HC-SR501 e il modulo vocale ISD1820.

IL MODULO ESP-01

Il modulo ESP-01 è un modulo Wi-Fi molto potente utilizzato principalmente nei progetti IoT. In **Figura 2** è riportato il layout e in **Figura 3** la piedinatura dell'ESP-01.

Il modulo ESP-01 ha al suo interno il microcontrollore ESP8266 sviluppato da Espressif Systems, un'azienda con sede a Shanghai. Questo microcontrollore ha la capacità di eseguire attività connesse al Wi-Fi, quindi è ampiamente utilizzato come dispositivo Wi-Fi program-

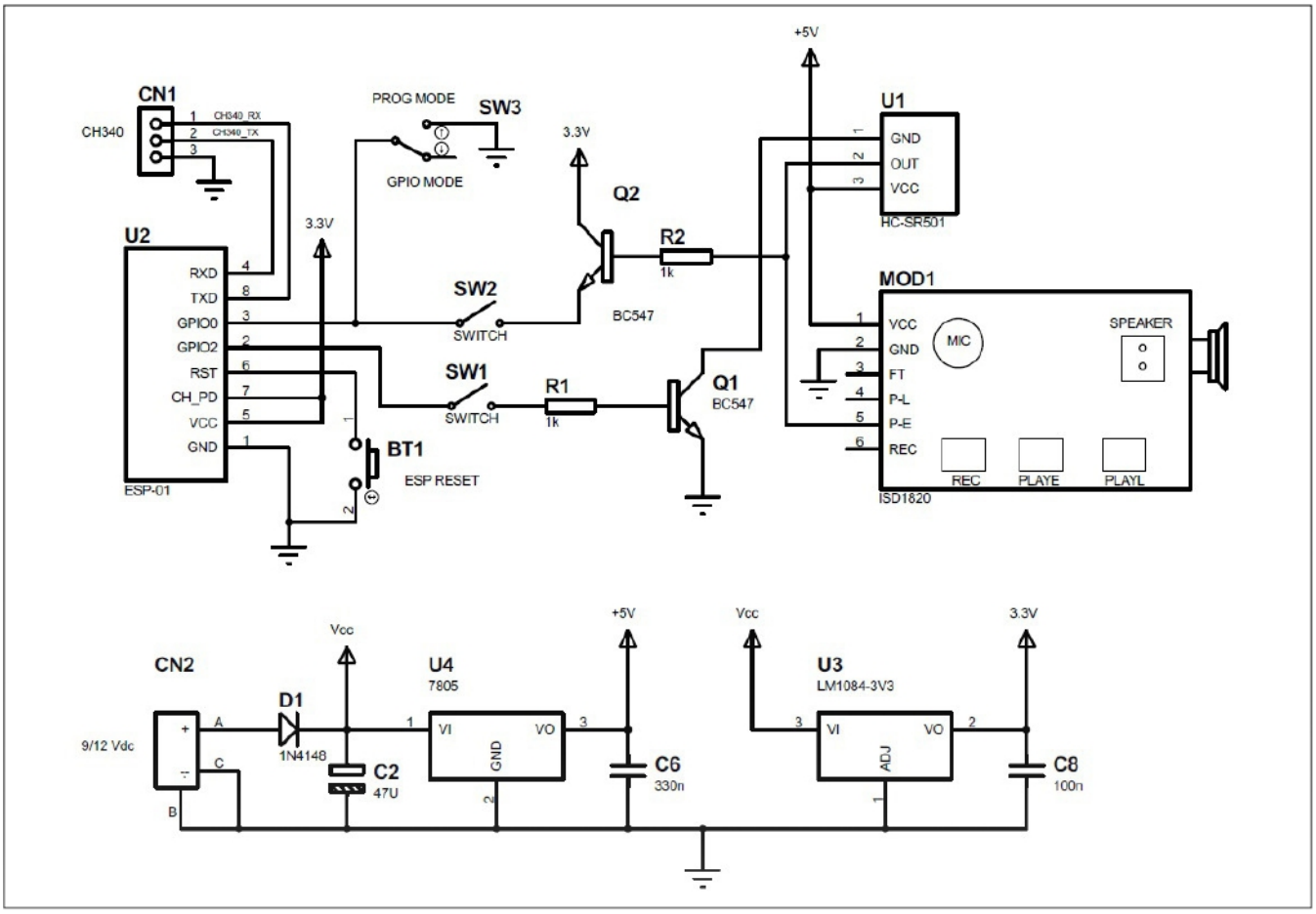


Figura 1: Schema elettrico del sistema di sicurezza IoT

mabile. Sono disponibili varie versioni di moduli ESP che integrano l'ESP8266, dall'ESP-01 all'ESP-12.

Quello che utilizzeremo nel nostro progetto è l'ESP-01 poiché è il più economico e facilmente disponibile. Tuttavia, tutti i moduli ESP hanno un solo tipo di processore ESP, ciò che differisce è solo il tipo di breakout board utilizzata.

La breakout board di ESP-01 ha solo 2 pin GPIO (**Gene-**

QUELLO CHE HAI LETTO E' UN ESTRATTO, L'ARTICOLO COMPLETO E' RISERVATO AGLI ABBONATI AD ELETTRONICA OPEN SOURCE.

PERCHE' ABBONARSI A PLATINUM 2.0?

UN ANNO DI **FIRMWARE 2.0**
TUTTI GLI ARTICOLI TECNICI RISERVATI
CONTEST E **PROMOZIONI** RISERVATI

VOGLIO ABBONARMI!

PROGETTO DI UN SISTEMA DI SICUREZZA IOT CON IL SENSORE PIR HC-SR501 – PARTE 2

di **Fulvio De Santis**

Nel precedente articolo "Progetto di un sistema di sicurezza IoT con il sensore PIR HC-SR501 - Parte 1" abbiamo descritto step-by-step il progetto ed i suoi componenti più rilevanti di un sistema di sicurezza IoT con allarme vocale basato sul sensore PIR HC-SR501, modulo Wi-Fi ESP-01 e modulo vocale ISD1820. Poi abbiamo anche creato un'API Gmail per l'invio di un'email di allarme tramite il modulo Wi-Fi ESP-01 del nostro progetto. In questo articolo tratteremo la seconda parte del progetto. Realizzeremo il circuito su una scheda sperimentale, creeremo uno sketch con l'IDE di Arduino in cui riporteremo il codice di gestione del sistema di sicurezza, descriveremo le parti più rilevanti di questo codice, infine faremo il test funzionale del progetto con cui constateremo la possibilità di attivare o disattivare il sistema da remoto via web, grazie ancora all'impiego del modulo Wi-Fi ESP-01.

INTRODUZIONE

Per chi non avesse letto la prima parte del progetto, ne ripetiamo la sintetica **descrizione della funzionalità del sistema di sicurezza IoT**.

"Questo sistema di sicurezza è in grado di attivare un messaggio audio di segnalazione di intrusione mediante il modulo vocale ISD1820 e nel contempo di inviare un'e-mail quando il sistema rileva la presenza di un intruso. Inoltre, il sistema di sicurezza può essere attivato/disattivato da remoto via Internet. Con il modulo vocale ISD1820 è possibile registrare una traccia audio di 10 secondi che verrà riprodotta quando viene rilevato il movimento di una persona. L'email di avviso di allarme intrusione viene inviata con data e ora dell'evento ad un predefinito indirizzo email."

Si tenga presente che il sistema di sicurezza presentato in questo articolo e nel precedente, deve essere considerato non prioritario ma ausiliario ad un sistema di sicurezza primario preesistente.

REALIZZAZIONE DEL PROGETTO

Realizzate il circuito del sistema di sicurezza eseguendo i collegamenti dello schema elettrico che riportiamo in **Figura 1** saldando i componenti su un circuito stampato che vorrete creare o su una scheda ramata millefori, oppure utilizzate una breadboard sperimentale e dei jumper. Consigliamo di utilizzare dei connettori berg stick femmina/maschio da inserire nella scheda in modo da evitare saldature sui moduli che collegherete con dei jumper ai terminali berg stick della scheda.

CREAZIONE DELLO SKETCH E PROGRAMMAZIONE DELL'ESP8266 CON L'IDE DI ARDUINO

Completata la realizzazione dell'hardware, ora andremo a creare uno sketch contenente il codice di gestione del sistema di sicurezza, che caricheremo (programmeremo) nella **memoria flash dell'ESP8266**. Il codice con cui andremo a programmare l'ESP8266 viene inserito in uno sketch utilizzando l'IDE di Arduino. Una delle funzioni del codice viene utilizzata per configurare l'ESP-01 come AP (Access Point) e STA (Station). Inoltre, viene creata una pagina Web utilizzando il codice HTML con cui è possibile Attivare/Disattivare il sistema di sicurezza.

CREAZIONE DELLO SKETCH

Innanzitutto occorre installare l'IDE di Arduino dal sito ufficiale www.arduino.cc (in questo articolo si fa riferimento

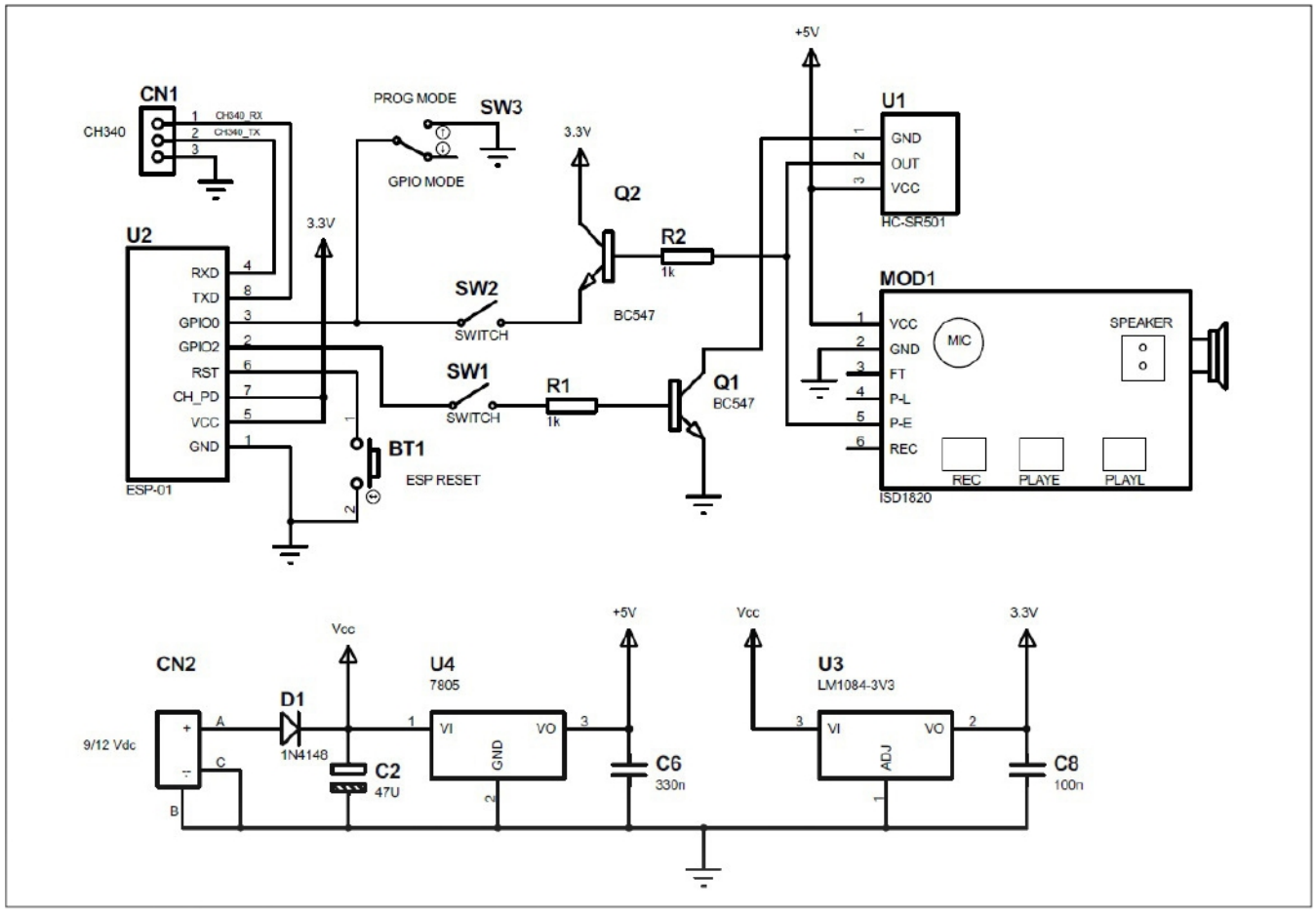


Figura 1: Schema elettrico del sistema di sicurezza IoT

alla versione software di Arduino 1.8.12). Avviate l'IDE di Arduino e in un nuovo sketch copiate il codice riportato di seguito e salvate lo sketch con il nome SistSicur_IoT, o come preferite.

```
#include <ESP8266WiFi.h>
#include <WiFiClient.h>
```

```
your password here

ESP8266WebServer server(80);

String mainPage = ""; //The default page
String feedback = ""; //Gives staus of the switch
```

QUELLO CHE HAI LETTO E' UN ESTRATTO, L'ARTICOLO
COMPLETO E' RISERVATO AGLI ABBONATI
AD ELETTRONICA OPEN SOURCE.

PERCHE' ABBONARSI A PLATINUM 2.0?

UN ANNO DI FIRMWARE 2.0
TUTTI GLI ARTICOLI TECNICI RISERVATI
CONTEST E PROMOZIONI RISERVATI

VOGLIO ABBONARMI!

+ 130.000
REGISTERED USERS

6.138 AVERAGE DAILY PAGEVIEWS (DEC2019)

824.057 2019 ANNUAL VISITORS

THE BIGGEST **EMBEDDED COMMUNITY** IN ITALY

SOCIAL CONNECTIONS

+ 83.000

+ 23.000

CATEGORIES

COMPANIES/CONSULTANTS
53 %

ACADEMICS/STUDENTS
25 %

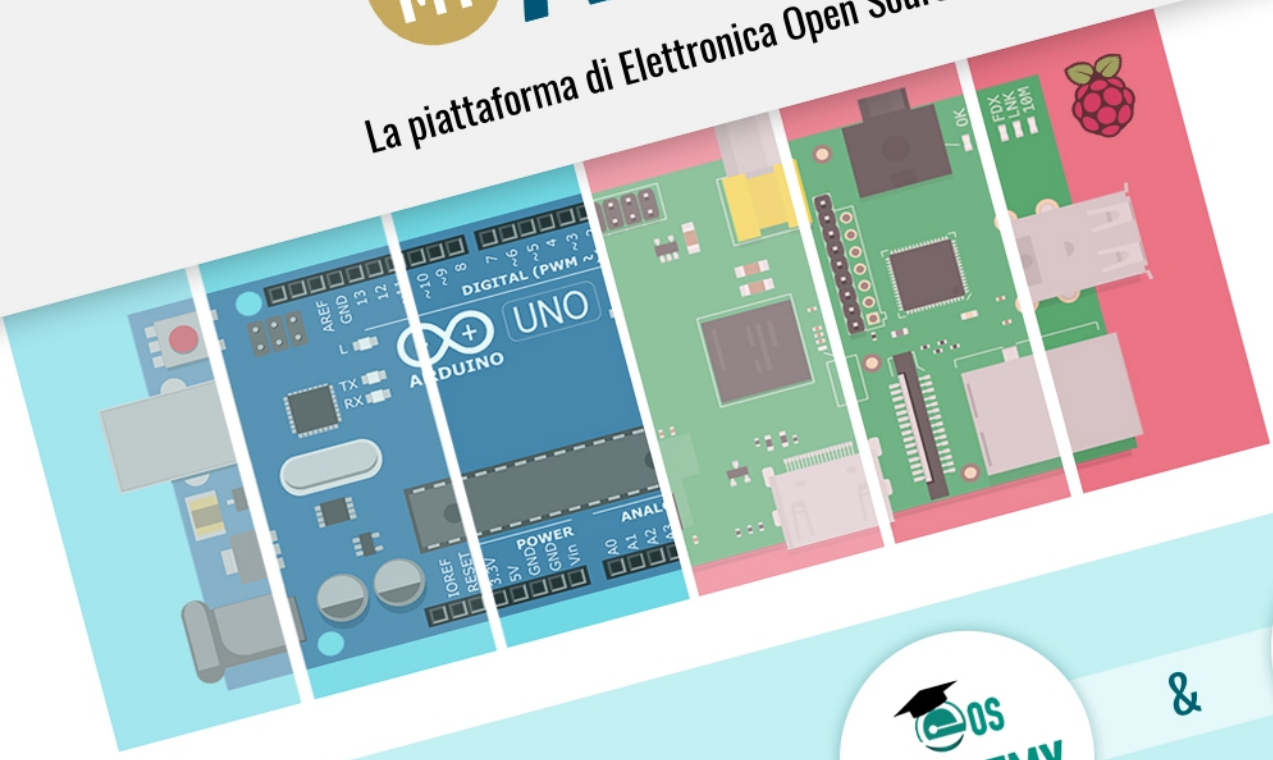
MAKERS/HOBBYISTS
22 %

Elettronica Open Source

I NOSTRI CORSI DI ELETTRONICA
PER I PROFESSIONISTI
E I MAKERS

MY ACADEMY

La piattaforma di Elettronica Open Source dedicata ai corsi



PUOI AVERE TUTTI I CORSI DI

OS ACADEMY

&

MAKERS ACADEMY

A PORTATA DI CLICK